

1 Table of Contents

Contents

1	Table of Contents.....	1
1.1	Revision History	2
2	ClearPass Switch Integration demo	3
2.1	Things you need.....	3
2.2	Demo/PoC Assumptions	3
2.3	Demonstration Goals	3
3	Windows Domain Controller	4
4	ClearPass Policy Manager.....	6
4.1	Joining AD Domain	6
4.2	Authentication Sources	7
4.3	Adding Network Access Device.....	9
4.4	Adding RADIUS Dictionary	9
5	Aruba Switch Configuration	11
5.1	VLAN and DHCP configuration	11
5.2	Policy Configuration	11
5.3	Authentication Configuration.....	13
5.4	NTP Configuration	14
6	ClearPass Services	16
6.1	Services - Ariya WiredAOS-S Dot1x	16
6.2	Enforcement Profiles.....	17
6.3	Dot1x Testing	17
6.4	Endpoint Attributes.....	21
6.5	Services - Ariya Wired-AOS-S Mac Auth	22
6.6	Enforcement Profiles.....	23
6.7	Services - Ariya Wired-AOS-S GuestWebAuth	24
6.8	Enforcement Profiles.....	26
6.9	ClearPass Guest Splash Page	27
7	Testing Captive Portal with MAC Auth	30
7.1	Guest User with Captive Portal with MAC Auth	30
7.2	AD User with Captive Portal with MAC Auth	35
7.3	Aruba Switch Captive Portal Redirection	39
8	Wired Enforcement for Instant APs Dot1x	42
8.1	Instant AP Configuration	42
8.2	Wired Dot1x Service Policy	43
8.3	LAN Switch Configuration	44
8.4	Testing	44
9	Wired Enforcement for Instant APs MAC Auth	49
9.1	Instant AP Configuration	49
9.2	Wired MAC Auth Service Policy.....	49
9.3	LAN Switch Configuration	50
9.4	Testing	50

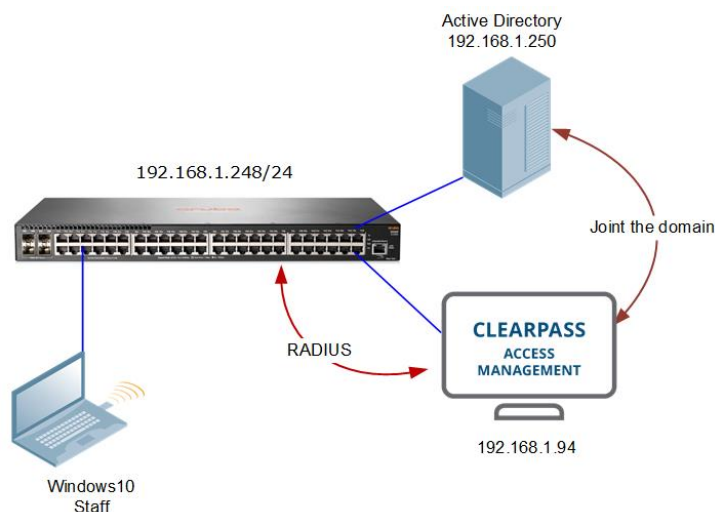
10	Wired Enforcement Critical Access.....	54
10.1	Aruba Switch Configuration	54
10.2	Testing	54
11	Wired Enforcement for IP Phones	57
11.1	Wired Dot1x Service Policy	57
11.2	Wired MAC Auth with Captive Portal Service Policy	58
12	Downloadable User Roles	62
12.1	ClearPass Service Configuration	62
12.2	Aruba Switch Configuration	64
12.3	Automatic Certificate download with ClearPass.....	65
12.4	DUR Testing	67
12.5	DUR with Captive Portal	69
12.6	DUR with Instant APs – dot1x	77
12.7	DUR with Instant APs – Profiling.....	80

1.1 Revision History

DATE	VERSION	EDITOR	CHANGES
14 March 2019	0.1	Ariya Parsamanesh	Initial creation
18 March 2019	0.2	Ariya Parsamanesh	Added the profiling section
19 March 2019	0.3	Ariya Parsamanesh	Minor updates

2 ClearPass Switch Integration demo

The main objective of these guides are for easy/quick demo of ClearPass Policy Manager (CPPM) wired dot1x, MAC authentication, Guest Captive portal and local/downloadable user roles for Aruba switches.



2.1 Things you need

- W2K8 as a Domain controller (VM) - 192.168.1.250/24
- ClearPass Policy Manager 6.7.9.(VM) - 192.168.1.94/24
- Aruba 2930F switch running WC.16.08.0001 - 192.168.1.248/24
- A laptop that can do dot1x authentication.
 - Staff user will be in Staff role using VLAN 10
 - Student user will be in Student role using VLAN 20

2.2 Demo/PoC Assumptions

- ClearPass should join the AD domain with an AD user account with Admin rights (have the user credentials ready)
- The DNS setting on the ClearPass (CP) should be able to resolve the AD NetBIOS name (generally the DNS should be AD)
- ClearPass needs Internet access to get the updates, the ClearPass network segment should be able to route to the Internet

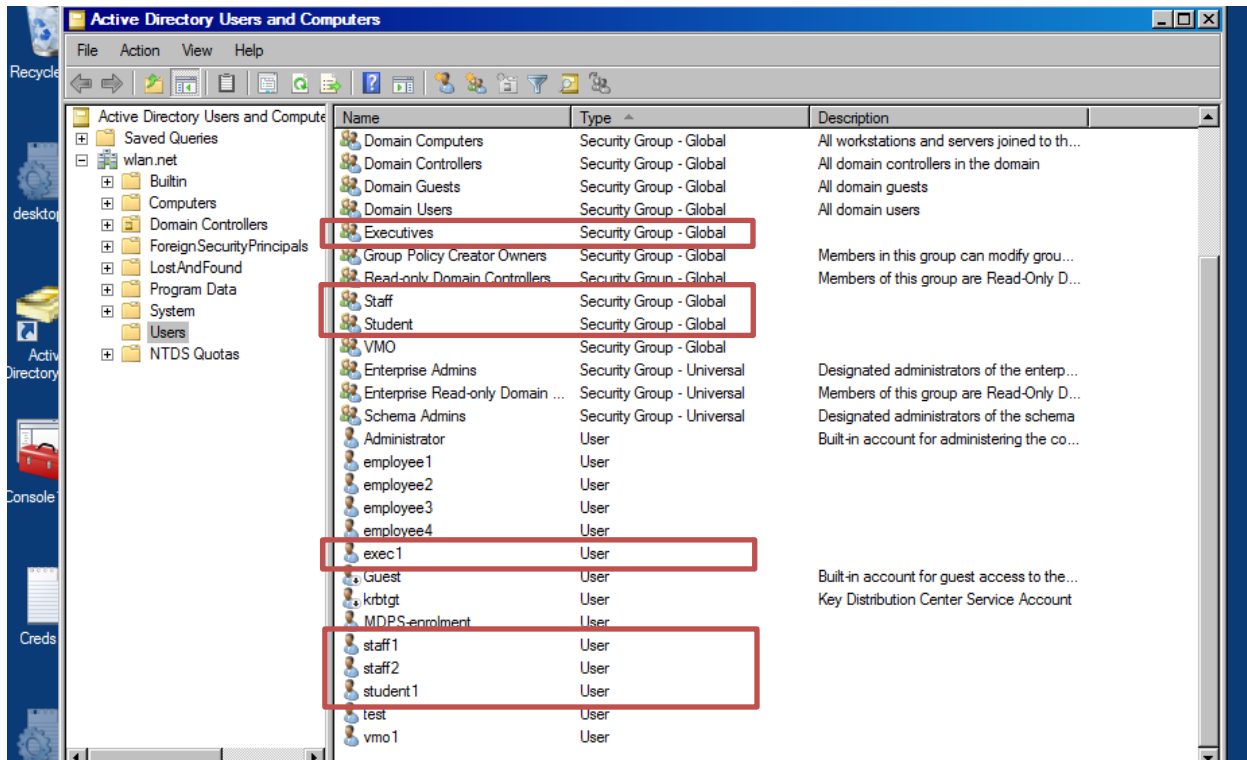
2.3 Demonstration Goals

- Performing wired dot1x with Aruba Switches using Local and Downloadable user roles
- AD based dot-1x authentication and user-role assignment for user being staff1, student1 and exec1
- MAC authentication and MAC caching with automatic captive portal redirection
- Profiling/MAC Auth and Dot1x authentication of Instant APs with Local and downloadable user roles

3 Windows Domain Controller

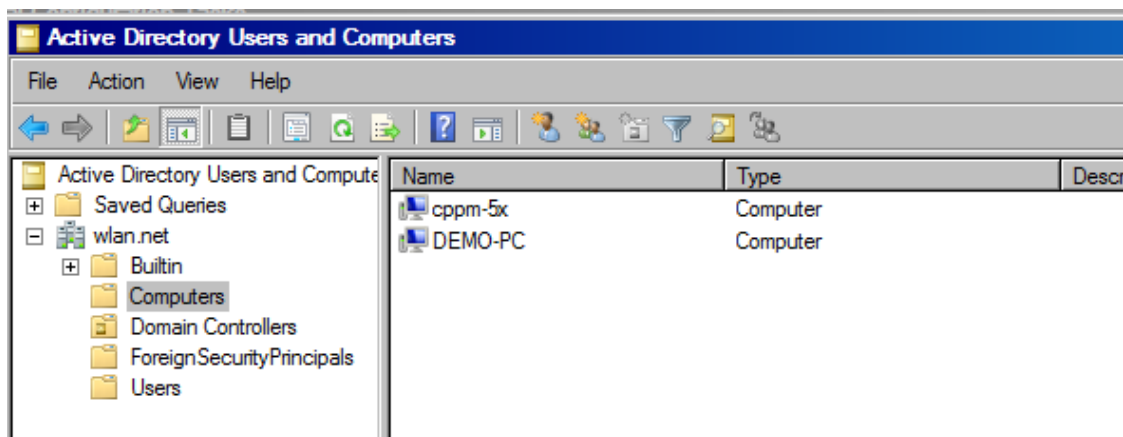
- Create relevant users and user groups
- Ensure that one of your laptops (domain laptop) has joined the domain using the LAN

Here we have connected to the DC and have three users groups (Staff, Student and Executives)



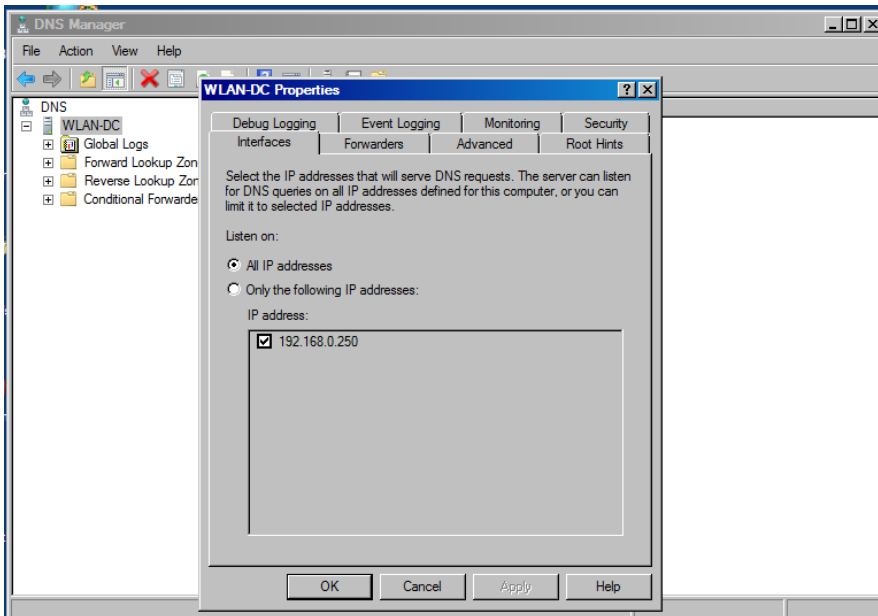
And the users in each of those groups are staff1/2, student1 and exec1.

The following screen shot shows the laptop I am using (DEMO-PC) that is part of the domain as well as CPPM which needs to join the domain in order to authenticate against Microsoft domain. I'll cover the CPPM side in the CPPM section.

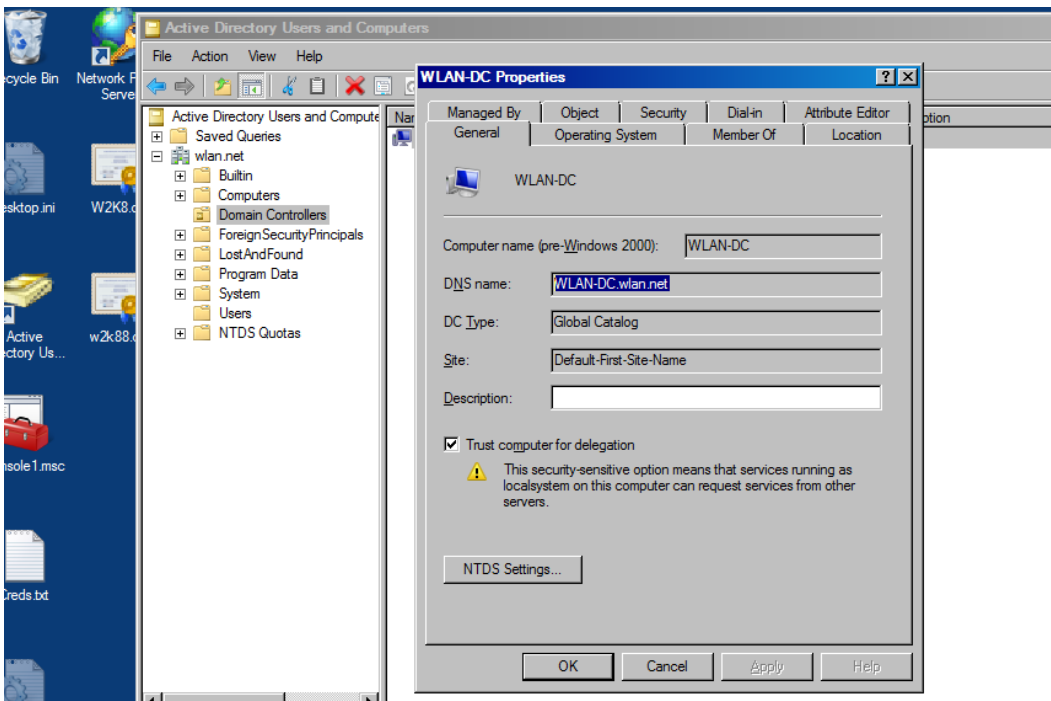


You also need to ensure you have DNS running on the DC.

Note: This is needed to for CPPM to join the domain.



Here the Domain controller's name is "WLAN-DC.wlan.net". We need this when we are configuring the CPPM joining the domain.



4 ClearPass Policy Manager

4.1 Joining AD Domain

Configure the IP addresses and the rest as per your Lab setup but ensure you have the IP address of your W2K8 DC as the primary DNS. CPPM needs to join the AD domain in order to authenticate against it.

Make sure the clock time for AD and CPPM are almost in sync. It is best to use NTP. If they are not in sync then CPPM will not be able to join the domain.

When you click on the "join domain" button, you need to provide the FQDN of the DC and that's why you need the DNS entry to resolve the name of your W2K8 DC.

Administration » Server Manager » Server Configuration - poc.clearpass.info

Server Configuration - poc.clearpass.info (192.168.1.94)

System Services Control Service Parameters System Monitoring Network FIPS

Master Server in Zone: Primary master

Span Port:

Join AD Domain

Enter the FQDN of the controller and the short (NETBIOS) name for the domain:

Domain Controller: wlan-dc.wlan.net

NetBIOS Name: WLAN

In case of a controller name conflict

☒ Use specified Domain Controller

☐ Use Domain Controller returned by DNS query

☐ Fail on conflict

☒ Use default domain admin user [Administrator]

Username: Administrator

Password: [REDACTED]

Save Cancel

Join AD Domain

Adding host to AD domain

Adding host to AD domain...

INFO - Fetched REALM 'WLAN.NET' from domain FQDN 'wlan-dc.wlan.net'

INFO - Fetched the NETBIOS name 'WLAN'

INFO - Creating domain directories for 'WLAN'

INFO - Using Administrator as the WLAN-DC's username

Enter Administrator's password:

Using short domain name -- WLAN

Joined 'CP63LAB' to dns domain 'wlan.net'

INFO - Creating service scripts for 'WLAN'

Starting cpass-domain-server_WLAN: [OK]

Close

Join AD Domain

Added host to the domain

INFO - Creating service scripts for 'WLAN'

Starting cpass-domain-server_WLAN: [OK]

INFO - updating domain configuration files

Stopping cpass-domain-server_WLAN: [OK]

Starting cpass-domain-server_WLAN: [OK]

Stopping cpass-sysmon-server: [OK]

Starting cpass-sysmon-server: [OK]

Stopping cpass-radius-server: [OK]

Starting cpass-radius-server: [OK]

INFO - CP63Lab joined the domain WLAN.NET

Close

The Admin user does require some elevated privileges. Joining the domain allows CPPM to authenticate 802.1x methods that have MSCHAPv2 as the inner-EAP method such as PEAP.

This join procedure is done ONCE and only ONCE. We do NOT save or cache the account used to join the node to AD.

When you are done, you can use a typical service account with a non-expiring password when you add AD as an authentication source. This account will not need the same elevated privilege level.

This is what you should get after ClearPass has successfully joined the domain. (The subnet masks for both the ports are deliberate as I have one interface on my VM server.)

System	Services Control	Service Parameters	System Monitoring	Network	FIPS
Master Server in Zone:		Primary master			
Span Port:		-- None --			
		IPv4	IPv6	Action	
Management Port	IP Address	192.168.1.94			Configure
	Subnet Mask	255.255.255.0			
	Default Gateway	192.168.1.249			
Data/External Port	IP Address				Configure
	Subnet Mask				
	Default Gateway				
DNS Settings	Primary	192.168.1.250			Configure
	Secondary	192.168.1.1			
	Tertiary				
	DNS Caching	Disabled			
AD Domains: Join AD Domain					
Domain Controller		NetBIOS Name	Password Servers	Action	
1.	WLAN.NET	WLAN	-		Leave AD Domain

4.2 Authentication Sources

You need to add the AD domain as an authentication source so CPPM can authenticate against it.

Configuration

- Start Here
- Services
- Authentication
 - Methods
 - Sources
- Identity
 - Single Sign-On (SSO)

Filter: Name contains
Go Clear Filter
Show 20 records

#	<input type="checkbox"/>	Name ▲	Type	Description
1.	<input type="checkbox"/>	[Admin User Repository]	Local SQL DB	Authenticate users against Policy Manager admin user database
2.	<input type="checkbox"/>	AriyaAD	Active Directory	
3.	<input type="checkbox"/>	[Blacklist User Repository]	Local SQL DB	Blacklist database with users who have exceeded bandwidth or session related limits

I changed the default value for Server timeout form 10 sec to 300 sec.

Summary	General	Primary	Attributes
Name:	AriyaAD		
Description:			
Type:	Active Directory		
Use for Authorization:	<input checked="" type="checkbox"/> Enable to use this Authentication Source to also fetch role mapping attributes		
Authorization Sources:	<div> <div></div> <div>Remove</div> <div>View Details</div> </div> <div>-- Select --</div>		
Server Timeout:	300	seconds	
Cache Timeout:	36000	seconds	
Backup Servers Priority:	<div> <div></div> <div>Move Up</div> <div>Move Down</div> </div> <div>Add Backup Remove</div>		

Summary	General	Primary	Attributes
Connection Details			
Hostname:	192.168.1.250		
Connection Security:	None		
Port:	389 (For secure connection, use 636)		
Verify Server Certificate:	<input checked="" type="checkbox"/> Enable to verify Server Certificate for secure connection		
Bind DN:	administrator@wlan.net (e.g. administrator@example.com OR cn=administrator,cn=users,dc=example,dc=com)		
Bind Password:	••••••••••		
NetBIOS Domain Name:	WLAN		
Base DN:	dc=wlan,dc=net		Search Base Dn
Search Scope:	SubTree Search		
LDAP Referrals:	<input type="checkbox"/> Follow referrals		
Bind User:	<input checked="" type="checkbox"/> Allow bind using user password		
User Certificate :	userCertificate		
Always use NETBIOS name:	<input type="checkbox"/> Enable to always use NETBIOS name instead of the domain part in username for authentication		

You can test the setup by clicking on the "Search Base Dn", which should bring up a LDAP browser and then you can basically walk the LDAP tree.

LDAP Browser	
Base DN:	dc=wlan,dc=net
dc=wlan,dc=net	<ul style="list-style-type: none"> CN=BuiltIn CN=Computers OU=Domain Controllers CN=ForeignSecurityPrincipals CN=Infrastructure CN=LostAndFound CN=NTDS Quotas CN=Program Data CN=System CN=Users
<div>Save Close</div>	

You should be able to click on the "Users" and see the users for this AD domain. Finally your AD authentication source should look like the following:

Authentication Sources - AriyaAD

Summary	General	Primary	Attributes
General:			
Name:	AriyaAD		
Description:			
Type:	AD		
Use for Authorization:	Enabled		
Authorization Sources:	-		
Primary:			
Hostname:	192.168.1.250		
Connection Security:	None		
Port:	389		
Verify Server Certificate:	true		
Bind DN:	administrator@wlan.net		
Bind Password:	*****		
NetBIOS Domain Name:	WLAN		
Base DN:	dc=wlan,dc=net		
Search Scope:	SubTree Search		
LDAP Referrals:	-		
Bind User:	true		
User Certificate :	userCertificate		
Always use NETBIOS name:	-		

Now to be able to provide differentiated user-role for onboard devices based on AD group, you need to ensure the Attributes are correctly configured. This is the default Attribute that should be already configured.

Summary	General	Primary	Attributes
Specify filter queries used to fetch authentication and authorization attributes			
Filter Name	Attribute Name	Alias Name	Enabled As
1. Authentication	dn	UserDN	-
	department	Department	-
	title	Title	-
	company	company	-
	memberOf	memberOf	-
	telephoneNumber	Phone	-
	mail	Email	-
	displayName	Name	-
2. Group	accountExpires	Account Expires	-
	cn	Groups	-
3. Machine	dNSHostName	HostName	-
	operatingSystem	OperatingSystem	-
	operatingSystemServicePack	OSServicePack	-
4. Onboard Device Owner	memberOf	Onboard memberOf	-
5. Onboard Device Owner Group	cn	Onboard Groups	-

4.3 Adding Network Access Device

Here we need to add the Aruba switch to CPPM as a NAD.

Edit Device Details

Device	SNMP Read Settings	SNMP Write Settings	CLI Settings	OnConnect Enforcement	Attributes
Name:	Aruba-2930F-Lab2				
IP or Subnet Address:	192.168.1.248 (e.g., 192.168.1.10 or 192.168.1.1/24 or 192.168.1.1-20)				
Description:					
RADIUS Shared Secret:			Verify:		
TACACS+ Shared Secret:			Verify:		
Vendor Name:	Hewlett-Packard-Enterpr				
Enable RADIUS CoA:	<input checked="" type="checkbox"/> RADIUS CoA Port: 3799				

Copy Save Cancel

4.4 Adding RADIUS Dictionary

Here we need to add the latest Hewlett-Packard-Enterprise RADIUS dictionary switch to CPPM. This can be download from the Aruba Support site. Or if you have ClearPass 6.7.x it is already added.

aruba

Dashboard
Monitoring
Configuration
Administration
ClearPass Portal
Users and Privileges
Server Manager
External Servers
Certificates
Dictionaries
RADIUS
TACACS+ Services
Fingerprints
Attributes
Applications
Context Server Actions
Ingress Events
Agents and Software Updates
Support

ClearPass Policy Manager
Support | Help | Logout
admin (Super Administrator)

Administration » Dictionaries » RADIUS
RADIUS Dictionaries
Import

Filter: Vendor Name contains enter Go Clear Filter
Show 10 records

#	Vendor Name	Vendor ID	Vendor Prefix	Enabled
1.	Alcatel-Lucent-Enterprise	800	Alcatel-Lucent-Enterprise	true
2.	Hewlett-Packard-Enterprise	11	Hewlett-Packard-Enterprise	true

Showing RADIUS Attributes

Vendor Name: Hewlett-Packard-Enterprise (11)

21.	HPE-Port-Bounce-Host	23	Unsigned32	in out
22.	HPE-Port-Dot1X-Client-Limit	10	Unsigned32	in out
23.	HPE-Port-Dot1X-Port-Mode	13	Unsigned32	in out
24.	HPE-Port-MACAuth-Client-Limit	11	Unsigned32	in out
25.	HPE-Port-MACAuth-Port-Mode	14	Unsigned32	in out
26.	HPE-Port-Priority-Regeneration-Table	40	String	in out
27.	HPE-Port-Speed	49	String	in out
28.	HPE-Port-Webauth-Client-Limit	12	Unsigned32	in out
29.	HPE-Privilege-Level	1	Unsigned32	in out
30.	HPE-Time	22	Time	in out
31.	HPE-User-Role	25	String	in out

Disable Export Close

Next we'll be creating the relevant ClearPass services.

5 Aruba Switch Configuration

Here we cover the Aruba 2930F switch configuration.

5.1 VLAN and DHCP configuration

Here we are enabling couple of VLANs and IP routing along with DHCP services.

```
ip route 0.0.0.0 0.0.0.0 192.168.1.1
ip routing

vlan 1
    name "DEFAULT_VLAN"
    no untagged 1-4
    untagged 5-10
    ip address dhcp-bootp
    exit
vlan 10
    name "Lab"
    untagged 3-4
    tagged 8
    ip address 10.10.10.1 255.255.255.0
    dhcp-server
    exit
vlan 20
    name "VLAN20"
    tagged 8
    ip address 10.10.20.1 255.255.255.0
    dhcp-server
    exit
vlan 192
    name "VLAN192"
    untagged 1-2
    tagged 8
    ip address 192.168.1.248 255.255.255.0
    exit

allow-unsupported-transceiver

dhcp-server pool "VLAN10"
    authoritative
    default-router "10.10.10.1"
    dns-server "8.8.8.8"
    network 10.10.10.0 255.255.255.0
    range 10.10.10.100 10.10.10.199
    exit

dhcp-server pool "VLAN20"
    default-router "10.10.20.1"
    dns-server "8.8.8.8"
    network 10.10.20.0 255.255.255.0
    range 10.10.20.100 10.10.20.199
    exit

dhcp-server enable

ip source-interface radius vlan 192
ip client-tracker
```

5.2 Policy Configuration

These "policy user" commands create a context that may be used to classify the policy. The new actions are specific to policy user are redirect, permit and deny.

```
class ipv4 "DHCP"
  10 match udp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 67
  Exit

class ipv4 "HOME-LAN"
  10 match ip 0.0.0.0 255.255.255.255 192.168.1.0 0.0.0.255
  Exit

class ipv4 "INTERNET"
  10 match ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
  Exit

class ipv4 "IP-ANY-ANY"
  10 match ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
  Exit

class ipv4 "WEB-TRAFFIC"
  10 match tcp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 80
  20 match tcp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 443
  Exit

class ipv4 "DNS-INTERNAL"
  10 match udp 0.0.0.0 255.255.255.255 192.168.1.1 0.0.0.0 eq 53
  exit
class ipv4 "CLEARPASS-WEB"
  30 match tcp 0.0.0.0 255.255.255.255 192.168.1.94 0.0.0.0 eq 80
  40 match tcp 0.0.0.0 255.255.255.255 192.168.1.94 0.0.0.0 eq 443
  Exit

policy user "CLEARPASS-REDIRECT"
  10 class ipv4 "DNS-INTERNAL" action permit
  20 class ipv4 "DHCP" action permit
  30 class ipv4 "CLEARPASS-WEB" action permit
  40 class ipv4 "WEB-TRAFFIC" action redirect captive-portal
  Exit

policy user "Staff"
  10 class ipv4 "HOME-LAN" action permit
  20 class ipv4 "INTERNET" action permit
  30 class ipv4 "IP-ANY-ANY" action permit
  exit

policy user "Students"
  10 class ipv4 "HOME-LAN" action permit
  20 class ipv4 "INTERNET" action permit
  30 class ipv4 "IP-ANY-ANY" action permit
  Exit

policy user "CORPORATE"
  10 class ipv4 "HOME-LAN" action permit
  20 class ipv4 "INTERNET" action permit
  Exit

policy user "GUEST"
  5 class ipv4 "DHCP" action permit
  10 class ipv4 "DNS-INTERNAL" action permit
  20 class ipv4 "HOME-LAN" action deny
  30 class ipv4 "INTERNET" action permit
  Exit

policy user "MAC-AUTH-CORP-USER"
  10 class ipv4 "DNS-INTERNAL" action permit
```

```
20 class ipv4 "HOME-LAN" action permit
30 class ipv4 "INTERNET" action permit
Exit
```

5.3 Authentication Configuration

```
radius-server host 192.168.1.94 key "aruba123"
radius-server host 192.168.1.94 dyn-authorization
radius-server host 192.168.1.94 time-window plus-or-minus-time-window
radius-server host 192.168.1.94 time-window 0

aaa server-group radius "ClearPass" host 192.168.1.94

aaa authorization user-role name "GUEST"
    reauth-period 3600
    vlan-id 10
    exit

aaa authorization user-role name "Employee"
    policy "CORP-USER"
    vlan-id 10
    exit

aaa authorization user-role name "Staff"
    policy "Staff"
    vlan-id 10
    exit

aaa authorization user-role name "Students"
    policy "Students"
    vlan-id 20
    exit

aaa authorization user-role name "MAC-AUTH-CORP"
    policy "MAC-AUTH-CORP-USER"
    vlan-id 192
    exit

aaa authorization user-role name "CAPTIVE-PORTAL"
    captive-portal-profile "use-radius-vs-a"
    policy "CLEARPASS-REDIRECT"
    reauth-period 180
    vlan-id 10
    exit

aaa accounting network start-stop radius server-group "ClearPass"
aaa authorization user-role enable download
aaa authentication port-access eap-radius server-group "ClearPass"
aaa authentication mac-based chap-radius server-group "ClearPass"
aaa authentication captive-portal enable

aaa port-access authenticator 4
aaa port-access authenticator 4 tx-period 10
aaa port-access authenticator 4 supplicant-timeout 10
aaa port-access authenticator 4 client-limit 5
aaa port-access authenticator active
aaa port-access mac-based 4
aaa port-access mac-based 4 addr-limit 5

aaa port-access 4 auth-order mac-based authenticator
aaa port-access 4 auth-priority authenticator mac-based
```

Note that "4" in the aaa port-access" commands refers to the switch port.
 We have enabled the new feature to provide the authentication order of a port.
 To check if your RADIUS server is working you can use the following commands.

```
Aruba-2930F-Lab2# show radius authentication

Status and Counters - RADIUS Authentication Information

NAS Identifier           : Aruba-2930F-Lab
Invalid Server Addresses : 0
UDP
Server IP Addr  Port  Timeouts  Requests  Challenges  Accepts  Rejects
-----
192.168.1.94    1812  19        28         11           12       0

Aruba-2930F-Lab2#
```

5.4 NTP Configuration

The Network Time Protocol (NTP) synchronizes the time of day among a set of distributed time servers and clients in order to correlate events when receiving system logs and other time-specific events from multiple network devices. The timezone we are using is 600 for NSW, Vic and ACT. This means 600 min ahead of GMT.

```
timesync sntp
sntp unicast
sntp server priority 1 216.239.35.4
sntp server priority 2 216.239.35.8
sntp server priority 3 216.239.35.12
time daylight-time-rule user-defined begin-date 10/01 end-date 04/02
time timezone 600
```

You can check the status of SNTP with these commands.

```
Aruba-2930F-Lab2# sh sntp

SNTP Configuration and Status

Time Sync Mode      : SNTP
SNTP Mode           : Unicast
Poll Interval (sec) : 720
SNTP Authentication : Disabled
Source IP Selection : Outgoing Interface

Priority SNTP Server Address          Version Key-id
-----
1      216.239.35.4                  3      0
2      216.239.35.8                  3      0
3      216.239.35.12                 3      0

Aruba-2930F-Lab2# sh sntp statistics

SNTP Statistics

Received Packets : 11
Sent Packets     : 11
Dropped Packets  : 0

SNTP Server Address          Auth Failed Pkts
-----
```

216.239.35.4	0
216.239.35.8	0
216.239.35.12	0

Aruba-2930F-Lab2#

AD-Group membership	Enforcement Profile	HPE-User-Role	
Staff	Ariya Wired-AOS-S-Staff	Staff	
Students	Ariya Wired-AOS-S-Students	Students	

6 ClearPass Services

We need to create minimum of three services as shown below.

6.	<input type="checkbox"/>	6	Ariya WiredAOS-S Dot1x	RADIUS	802.1X Wired	
7.	<input type="checkbox"/>	7	Ariya Wired-AOS-S MAC Auth	RADIUS	MAC Authentication	
8.	<input type="checkbox"/>	8	Ariya Wired-AOS-S GuestWebAuth	WEBAUTH	Web-based Authentication	

6.1 Services - Ariya WiredAOS-S Dot1x

Summary	Service	Authentication	Roles	Enforcement
Service:				
Name:	Ariya WiredAOS-S Dot1x			
Description:	802.1X Wired Access Service			
Type:	802.1X Wired			
Status:	Enabled			
Monitor Mode:	Disabled			
More Options:	-			
Service Rule				
Match ALL of the following conditions:				
Type	Name	Operator	Value	
1. Radius:IETF	NAS-Port-Type	EQUALS	Ethernet (15)	
2. Radius:IETF	Service-Type	BELONGS_TO	Login-User (1), Framed-User (2), Authenticate-Only (8)	
3. Radius:IETF	Connect-Info	CONTAINS	CONNECT	
Authentication:				
Authentication Methods:	1. [EAP PEAP] 2. [EAP TLS]			
Authentication Sources:	AriyaAD			
Strip Username Rules:	-			
Service Certificate:	-			

Summary	Service	Authentication	Roles	Enforcement
Authentication Methods:				
[EAP PEAP] [EAP TLS]		<div>Move Up Move Down Remove View Details Modify</div>		Add new Authentication Method
--Select to Add--				
Authentication Sources:				
AriyaAD [Active Directory]		<div>Move Up Move Down Remove View Details Modify</div>		Add new Authentication Source
--Select to Add--				
Strip Username Rules: <input type="checkbox"/> Enable to specify a comma-separated list of rules to strip username prefixes or suffixes				

Summary	Service	Authentication	Roles	Enforcement		
Role Mapping Policy:						
--Select--		<div>Modify</div>		Add new Role Mapping Policy		
Role Mapping Policy Details						
Description:	-					
Default Role:	-					
Rules Evaluation Algorithm:	-					
<table><thead><tr><th>Conditions</th><th>Role</th></tr></thead></table>					Conditions	Role
Conditions	Role					

Summary	Service	Authentication	Roles	Enforcement
Use Cached Results: <input type="checkbox"/> Use cached Roles and Posture attributes from previous sessions				
Enforcement Policy:		Ariya Wired-AOS-S Dot1xEnforcementPolicy		Add new Enforcement Policy
Enforcement Policy Details				
Description:				
Default Profile:		[Deny Access Profile]		
Rules Evaluation Algorithm: first-applicable				
Conditions		Enforcement Profiles		
1. (Authorization:AriyaAD:memberOf CONTAINS staff)		Ariya Wired-AOS-S-Staff, [Update Endpoint Known]		
2. (Authorization:AriyaAD:memberOf CONTAINS Stude)		Ariya Wired-AOS-S-Students, [Update Endpoint Known]		

The default profile can be a default role such as the one we are using above or can be [deny all]

6.2 Enforcement Profiles

Enforcement Profiles - Ariya Wired-AOS-S-Staff

Summary	Profile	Attributes
Profile:		
Name:	Ariya Wired-AOS-S-Staff	
Description:		
Type:	RADIUS	
Action:	Accept	
Device Group List:	-	
Attributes:		
Type	Name	Value
1. Radius:Hewlett-Packard-Enterprise	HPE-User-Role	= Staff
2. Radius:IETF	Session-Timeout	= 86400

Enforcement Profiles - Ariya Wired-AOS-S-Students

Summary	Profile	Attributes
Profile:		
Name:	Ariya Wired-AOS-S-Students	
Description:		
Type:	RADIUS	
Action:	Accept	
Device Group List:	-	
Attributes:		
Type	Name	Value
1. Radius:Hewlett-Packard-Enterprise	HPE-User-Role	= Students
2. Radius:IETF	Session-Timeout	= 86400

[Update Endpoint Known]

Summary	Profile	Attributes
Profile:		
Name:	[Update Endpoint Known]	
Description:	System-defined profile to change Endpoint's status to Known	
Type:	Post_Authentication	
Action:		
Device Group List:	-	
Attributes:		
Type	Name	Value
1. Status-Update	Endpoint	= Known

6.3 Dot1x Testing

After a successful authentication the users should be placed in the following VLANs

User Groups	VLAN	User Role
Staff	10	Staff
Students	20	Students

Before we start let's have a look at configured user-roles.

```
Aruba-2930F-Lab2# show user-role
```

Downloaded user roles are preceded by *

User Roles

Enabled : Yes
Initial Role : denyall

Type	Name
------	------

local	GUEST
predefined	denyall
local	CORP-USER
local	MAC-AUTH-CORP
local	CAPTIVE-PORTAL

Aruba-2930F-Lab#

Aruba-2930F-Lab# sh port-access clients

Downloaded user roles are preceded by *

Port Access Client Status

Port	Client Name	MAC Address	IP Address	User Role	Type	VLAN
------	-------------	-------------	------------	-----------	------	------

Aruba-2930F-Lab#

We'll now connect a laptop to port 4 of the switch and start testing the dot1x PEAP authentication. This is the staff member authenticating.

Monitoring » Live Monitoring » Access Tracker

Access Tracker Jan 07, 2019 15:58:56 AEDT

Auto Refresh

The Access Tracker page provides a real-time display of per-session access activity on the selected server or domain.

[All Requests] poc.clearpass.info (192.168.1.94) Last 1 day before Today Edit

Filter: Request ID contains + Go Clear Filter Show 20 records

#	Server	Source	Username	Service	Login Status	Request Timestamp
1.	192.168.1.94	RADIUS	staff1	Ariya WiredAOS-S Dot1x	ACCEPT	2019/01/07 15:58:28

Alt

#	Server	Source	Username	Service	Login Status	Request Timestamp
1.	192.168.1.94	RADIUS	exec1	Ariya WiredAOS-S Dot1x	ACCEPT	2018/03/30 15:17:39
2.	192.168.1.94	RADIUS	staff1	Ariya WiredAOS-S Dot1x	ACCEPT	2018/03/30 15:08:51
3.	192.168.1.94	RADIUS	student1	Ariya WiredAOS-S Dot1x	ACCEPT	2018/03/30 13:51:37

Summary	Input	Output	Accounting
Login Status:	ACCEPT		
Session Identifier:	R00000000-01-5c32dc74		
Date and Time:	Jan 07, 2019 15:58:28 AEDT		
End-Host Identifier:	f0-de-f1-64-0a-82		
Username:	staff1		
Access Device IP/Port:	192.168.1.248:4 (Aruba-2930F-Lab2 / Hewlett-Packard-Enterprise)		
System Posture Status:	UNKNOWN (100)		
Policies Used -			
Service:	Ariya WiredAOS-S Dot1x		
Authentication Method:	EAP-PEAP,EAP-MSCHAPv2 ←		
Authentication Source:	AD:192.168.1.250		
Authorization Source:	AriyaAD		
Roles:	[User Authenticated]		
Enforcement Profiles:	[Update Endpoint Known], Ariya Wired-AOS-S-Staff ←		
Service Monitor Mode:	Disabled		
◀ ◀ Showing 1 of 1-2 records ▶ ▶ Change Status Show Configuration Export Show Logs Close			

Summary	Input	Output	Accounting
Username:	staff1		
End-Host Identifier:	f0-de-f1-64-0a-82		
Access Device IP/Port:	192.168.1.248:4 (Aruba-2930F-Lab2 / Hewlett-Packard-Enterprise)		
RADIUS Request			
Authorization Attributes			
Authorization:AriyaAD:Account Expires	9223372036854775807 [30828-09-14 12:48:05 AEST]		
Authorization:AriyaAD:memberOf	CN=Administrators,CN=Builtin,DC=wlan,DC=net, CN=Staff,CN=Users,DC=wlan,DC=net ←		
Authorization:AriyaAD:Name	staff1		
Authorization:AriyaAD:UserDN	CN=staff1,CN=Users,DC=wlan,DC=net		
Computed Attributes			

Summary	Input	Output	Accounting
Enforcement Profiles:	[Update Endpoint Known], Ariya Wired-AOS-S-Staff		
System Posture Status:	UNKNOWN (100)		
Audit Posture Status:	UNKNOWN (100)		
RADIUS Response			
Radius:Hewlett-Packard-Enterprise:HPE-User-Role	Staff		
Radius:IETF:Session-Timeout	86400		
Status-Update:Endpoint	Known		

Since ClearPass indicated a successful dot1x authentication along with sending RADIUS HPE-User-Role, we should see the corresponding user-role on the Aruba 2930F switch.

```
Aruba-2930F-Lab2# sh port-access client
Downloaded user roles are preceded by *
```

Port Access Client Status

Port	Client Name	MAC Address	IP Address	User Role	Type	VLAN
4	staff1	f0def1-640a82	10.10.10.100	Staff	8021X	10

```
Aruba-2930F-Lab2#
```

And now if we login with a different AD user like student1 who is not in the staff user group, after successful authentication it will be put into a different VLAN along with different policy.

Monitoring » Live Monitoring » Access Tracker


Access Tracker Jan 07, 2019 16:21:15 AEDT

 Auto Refresh

The Access Tracker page provides a real-time display of per-session access activity on the selected server or domain.

 [All Requests]
  poc.clearpass.info (192.168.1.94)
  Last 1 day before Today
 [Edit](#)

Filter: Request ID contains [Go](#) [Clear Filter](#) Show 20 records

#	Server	Source	Username	Service	Login Status	Request Timestamp
1.	192.168.1.94	RADIUS	student1	Ariya WiredAOS-S Dot1x	ACCEPT 	2019/01/07 16:20:49
2.	192.168.1.94	RADIUS	staff1	Ariya WiredAOS-S Dot1x	ACCEPT	2019/01/07 15:58:28

Summary	Input	Output	Accounting
Login Status:	ACCEPT		
Session Identifier:	R00000001-01-5c32e1b0		
Date and Time:	Jan 07, 2019 16:20:49 AEDT		
End-Host Identifier:	f0-de-f1-64-0a-82		
Username:	student1		
Access Device IP/Port:	192.168.1.248:4 (Aruba-2930F-Lab2 / Hewlett-Packard-Enterprise)		
System Posture Status:	UNKNOWN (100)		
Policies Used -			
Service:	Ariya WiredAOS-S Dot1x		
Authentication Method:	EAP-PEAP,EAP-MSCHAPv2 ←		
Authentication Source:	AD:192.168.1.250		
Authorization Source:	AriyaAD		
Roles:	[User Authenticated]		
Enforcement Profiles:	[Update Endpoint Known], Ariya Wired-AOS-S-Students ←		
Service Monitor Mode:	Disabled		

Summary	Input	Output	Accounting
Enforcement Profiles:	[Update Endpoint Known], Ariya Wired-AOS-S-Students		
System Posture Status:	UNKNOWN (100)		
Audit Posture Status:	UNKNOWN (100)		

RADIUS Response	
Radius:Hewlett-Packard-Enterprise:HPE-User-Role	Students ←
Radius:IETF:Session-Timeout	86400
Status-Update:Endpoint	Known

```
Aruba-2930F-Lab2# sh port-access clients
Downloaded user roles are preceded by *
```

Port Access Client Status

Port	Client Name	MAC Address	IP Address	User Role	Type	VLAN
4	student1	f0def1-640a82	10.10.20.100	Students	8021X	20

```
Aruba-2930F-Lab2#
```

6.4 Endpoint Attributes

Here we need to create an endpoint attribute called "HPE_CompanyAsset", under the dictionary section, so that we can make use of it in the Role-mapping that we'll use in the next service.

Attributes

Filter: Name contains ass

#	Edit Attribute	
1		
2	Entity	Endpoint
	Name	HPE_CompanyAsset
	Data Type	Boolean
	Is Mandatory	<input checked="" type="radio"/> Yes <input type="radio"/> No
	Default Value (optional)	<input type="radio"/> True <input checked="" type="radio"/> False (e.g., true / false)
	<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

Now the attribute ' HPE_CompanyAsset' is available as ClearPass Attribute "HPE_CompanyAsset" and can be referenced as %{Endpoint:HPE_CompanyAsset}.

6.5 Services - Ariya Wired-AOS-S Mac Auth

Summary	Service	Authentication	Authorization	Roles	Enforcement
Service:					
Name:	Ariya Wired-AOS-S MAC Auth				
Description:	MAC-based Authentication Service				
Type:	MAC Authentication				
Status:	Enabled				
Monitor Mode:	Disabled				
More Options:	Authorization				
Service Rule					
Match ALL of the following conditions:					
Type	Name	Operator	Value		
1. Radius:IETF	NAS-Port-Type	BELONGS_TO	Ethernet (15), Wireless-802.11 (19)		
2. Radius:IETF	Service-Type	BELONGS_TO	Login-User (1), Call-Check (10)		
3. Connection	Client-Mac-Address	EQUALS	%{Radius:IETF:User-Name}		
4. Radius:IETF	Connect-Info	CONTAINS	CONNECT		
Authentication:					
Authentication Methods:	[Allow All MAC AUTH]				
Authentication Sources:	[Endpoints Repository]				
Strip Username Rules:	-				

Summary	Service	Authentication	Authorization	Roles	Enforcement
Authentication Methods:	<div> <div>[Allow All MAC AUTH]</div> <div> <input type="button" value="Move Up"/> <input type="button" value="Move Down"/> <input type="button" value="Remove"/> <input type="button" value="View Details"/> <input type="button" value="Modify"/> </div> </div> <div>--Select to Add--</div>				Add new Authentication Method
Authentication Sources:	<div> <div>[Endpoints Repository] [Local SQL DB]</div> <div> <input type="button" value="Move Up"/> <input type="button" value="Move Down"/> <input type="button" value="Remove"/> <input type="button" value="View Details"/> <input type="button" value="Modify"/> </div> </div> <div>--Select to Add--</div>				Add new Authentication Source
Strip Username Rules:	<input type="checkbox"/> Enable to specify a comma-separated list of rules to strip username prefixes or suffixes				

Summary	Service	Authentication	Authorization	Roles	Enforcement								
Authorization Details:													
Authorization sources from which role mapping attributes are fetched (for each Authentication Source)													
<table border="1"> <thead> <tr> <th>Authentication Source</th> <th>Attributes Fetched From</th> </tr> </thead> <tbody> <tr> <td>1. [Endpoints Repository] [Local SQL DB]</td> <td>[Endpoints Repository] [Local SQL DB]</td> </tr> </tbody> </table>						Authentication Source	Attributes Fetched From	1. [Endpoints Repository] [Local SQL DB]	[Endpoints Repository] [Local SQL DB]				
Authentication Source	Attributes Fetched From												
1. [Endpoints Repository] [Local SQL DB]	[Endpoints Repository] [Local SQL DB]												
Additional authorization sources from which to fetch role-mapping attributes -													
<table border="1"> <tbody> <tr> <td>[Insight Repository] [Local SQL DB]</td> <td rowspan="4"> <div> Remove View Details Modify </div> </td> </tr> <tr> <td>[Time Source] [Local SQL DB]</td> </tr> <tr> <td>[Guest User Repository] [Local SQL DB]</td> </tr> <tr> <td>[Guest Device Repository] [Local SQL DB]</td> </tr> <tr> <td colspan="2">--Select to Add--</td> <td></td> </tr> </tbody> </table>						[Insight Repository] [Local SQL DB]	<div> Remove View Details Modify </div>	[Time Source] [Local SQL DB]	[Guest User Repository] [Local SQL DB]	[Guest Device Repository] [Local SQL DB]	--Select to Add--		
[Insight Repository] [Local SQL DB]	<div> Remove View Details Modify </div>												
[Time Source] [Local SQL DB]													
[Guest User Repository] [Local SQL DB]													
[Guest Device Repository] [Local SQL DB]													
--Select to Add--													
Add new Authentication Source													

Summary	Service	Authentication	Authorization	Roles	Enforcement												
Role Mapping Policy:																	
Ariya Wired-AOS-S-MAC Auth-Role-Mapping Modify Add new Role Mapping Policy																	
Role Mapping Policy Details																	
Description:																	
Default Role: [Other]																	
Rules Evaluation Algorithm: evaluate-all																	
<table border="1"> <thead> <tr> <th>Conditions</th> <th>Role</th> </tr> </thead> <tbody> <tr> <td>1. (Authorization:[Endpoints Repository]:Unique-Device-Count EXISTS) AND (Date:Date-Time LESS_THAN %(Endpoint:MAC-Auth Expiry))</td> <td>[MAC Caching]</td> </tr> <tr> <td>2. (Endpoint:Guest Role ID EQUALS 1)</td> <td>[Contractor]</td> </tr> <tr> <td>3. (Endpoint:Guest Role ID EQUALS 2)</td> <td>[Guest]</td> </tr> <tr> <td>4. (Endpoint:Guest Role ID EQUALS 3)</td> <td>[Employee]</td> </tr> <tr> <td>5. (Authorization:[Endpoints Repository]:Status EQUALS known) OR (Endpoint:HPE_CompanyAsset EQUALS true)</td> <td>HPE_CompanyAsset</td> </tr> </tbody> </table>						Conditions	Role	1. (Authorization:[Endpoints Repository]:Unique-Device-Count EXISTS) AND (Date:Date-Time LESS_THAN %(Endpoint:MAC-Auth Expiry))	[MAC Caching]	2. (Endpoint:Guest Role ID EQUALS 1)	[Contractor]	3. (Endpoint:Guest Role ID EQUALS 2)	[Guest]	4. (Endpoint:Guest Role ID EQUALS 3)	[Employee]	5. (Authorization:[Endpoints Repository]:Status EQUALS known) OR (Endpoint:HPE_CompanyAsset EQUALS true)	HPE_CompanyAsset
Conditions	Role																
1. (Authorization:[Endpoints Repository]:Unique-Device-Count EXISTS) AND (Date:Date-Time LESS_THAN %(Endpoint:MAC-Auth Expiry))	[MAC Caching]																
2. (Endpoint:Guest Role ID EQUALS 1)	[Contractor]																
3. (Endpoint:Guest Role ID EQUALS 2)	[Guest]																
4. (Endpoint:Guest Role ID EQUALS 3)	[Employee]																
5. (Authorization:[Endpoints Repository]:Status EQUALS known) OR (Endpoint:HPE_CompanyAsset EQUALS true)	HPE_CompanyAsset																

Summary	Service	Authentication	Authorization	Roles	Enforcement								
Use Cached Results: <input type="checkbox"/> Use cached Roles and Posture attributes from previous sessions													
Enforcement Policy: Ariya Wired-AOS-S-MAC-Auth EnforcementPolic Modify Add new Enforcement Policy													
Enforcement Policy Details													
Description:													
Default Profile: Ariya Wired-AOS-S-Guest CaptivePortal													
Rules Evaluation Algorithm: first-applicable													
<table border="1"> <thead> <tr> <th>Conditions</th> <th>Enforcement Profiles</th> </tr> </thead> <tbody> <tr> <td>1. (Tips:Role EQUALS HPE_CompanyAsset)</td> <td>Ariya Wired-AOS-S-CorpDevice</td> </tr> <tr> <td>2. [User Authenticated] [Guest] (Tips:Role MATCHES_ALL [MAC Caching])</td> <td>Ariya Wired-AOS-S-MAC-Auth Guest, Ariya Return-Endpoint-Username</td> </tr> <tr> <td>3. AND (Tips:Role EQUALS [MAC Caching]) (Endpoint:Guest Role ID EQUALS AD-User)</td> <td>Ariya Wired-AOS-S-AD-Guest, Ariya Return-Endpoint-Username</td> </tr> </tbody> </table>						Conditions	Enforcement Profiles	1. (Tips:Role EQUALS HPE_CompanyAsset)	Ariya Wired-AOS-S-CorpDevice	2. [User Authenticated] [Guest] (Tips:Role MATCHES_ALL [MAC Caching])	Ariya Wired-AOS-S-MAC-Auth Guest, Ariya Return-Endpoint-Username	3. AND (Tips:Role EQUALS [MAC Caching]) (Endpoint:Guest Role ID EQUALS AD-User)	Ariya Wired-AOS-S-AD-Guest, Ariya Return-Endpoint-Username
Conditions	Enforcement Profiles												
1. (Tips:Role EQUALS HPE_CompanyAsset)	Ariya Wired-AOS-S-CorpDevice												
2. [User Authenticated] [Guest] (Tips:Role MATCHES_ALL [MAC Caching])	Ariya Wired-AOS-S-MAC-Auth Guest, Ariya Return-Endpoint-Username												
3. AND (Tips:Role EQUALS [MAC Caching]) (Endpoint:Guest Role ID EQUALS AD-User)	Ariya Wired-AOS-S-AD-Guest, Ariya Return-Endpoint-Username												

6.6 Enforcement Profiles

Here the configuration of the enforcement profiles that were referenced in the enforcement policy.

Ariya Wired-AOS-S-CorpDevice

Summary	Profile	Attributes
Profile:		
Name: Ariya Wired-AOS-S-CorpDevice		
Description:		
Type: RADIUS		
Action: Accept		
Device Group List: -		
Attributes:		
Type	Name	Value
1. Radius:Hewlett-Packard-Enterprise	HPE-User-Role	= CORP-DEVICE
2. Radius:IETF	Session-Timeout	= 86400

Ariya Wired-AOS-S-MAC-Auth Guest

Summary	Profile	Attributes
Profile:		
Name:	Ariya Wired-AOS-S-MAC-Auth Guest	
Description:		
Type:	RADIUS	
Action:	Accept	
Device Group List:	-	
Attributes:		
Type	Name	Value
1. Radius:Hewlett-Packard-Enterprise	HPE-User-Role	= GUEST
2. Radius:IETF	Session-Timeout	= 86400

Ariya Wired-AOS-S-AD-Guest

Summary	Profile	Attributes
Profile:		
Name:	Ariya Wired-AOS-S-AD-Guest	
Description:		
Type:	RADIUS	
Action:	Accept	
Device Group List:	-	
Attributes:		
Type	Name	Value
1. Radius:Hewlett-Packard-Enterprise	HPE-User-Role	= AD-Guest
2. Radius:IETF	Session-Timeout	= 86400

Ariya Return-Endpoint-Username

Summary	Profile	Attributes
Profile:		
Name:	Ariya Return-Endpoint-Username	
Description:		
Type:	RADIUS	
Action:	Accept	
Device Group List:	-	
Attributes:		
Type	Name	Value
1. Radius:IETF	User-Name	= %{Endpoint:Username}

The above enforcement profile is used to send back the username to the Aruba switch so that when you use show commands you can see the user name as well.

Ariya Wired-AOS-S-Guest CaptivePortal





Summary	Profile	Attributes
Profile:		
Name:	Ariya Wired-AOS-S-Guest CaptivePortal	
Description:		
Type:	RADIUS	
Action:	Accept	
Device Group List:	-	
Attributes:		
Type	Name	Value
1. Radius:Hewlett-Packard-Enterprise	HPE-User-Role	= CAPTIVE-PORTAL
2. Radius:Hewlett-Packard-Enterprise	HPE-Captive-Portal-URL	= https://192.168.1.94/guest/wired_guest.php
3. Radius:IETF	Session-Timeout	= 600

6.7 Services - Ariya Wired-AOS-S GuestWebAuth

With Aruba switches, we should use server-initiated workflow. This also makes the enforcement policy for the WEBAUTH quite simple. The main aim here is to update the endpoint database with some attributes that will be used for subsequent MAC authentications and then bounce the port to trigger a

re-authentication event and perhaps VLAN change and for the client to request a new IP address.

If a VLAN change is not required, a Terminate Session disconnect message can be used instead of a Bounce-Switch-Port.

Summary	Service	Authentication	Authorization	Roles	Enforcement
Name:	Ariya Wired-AOS-S GuestWebAuth				
Description:					
Type:	Web-based Authentication				
Status:	Enabled				
Monitor Mode:	<input type="checkbox"/> Enable to monitor network access without enforcement				
More Options:	<input checked="" type="checkbox"/> Authorization <input type="checkbox"/> Posture Compliance				
Service Rule					
Matches <input checked="" type="radio"/> ANY or <input type="radio"/> ALL of the following conditions:					
	Type	Name	Operator	Value	
1.	Host	CheckType	MATCHES_ANY	Authentication	 
2.	Application:ClearPass	Page-Name	EQUALS	wired-school	 
3.	Click to add...				

Note that second service rule, is only available in ClearPass 6.7.x

Summary	Service	Authentication	Authorization	Roles	Enforcement	
Authentication Sources:						
		<div>[Guest User Repository] [Local SQL DB] AriyaAD [Active Directory]</div> <div><div>Move Up</div><div>Move Down</div><div>Remove</div><div>View Details</div><div>Modify</div></div> <div>--Select to Add--</div>			Add new Authentication Source	
Strip Username Rules: <input type="checkbox"/> Enable to specify a comma-separated list of rules to strip username prefixes or suffixes						

Summary	Service	Authentication	Authorization	Roles	Enforcement						
Authorization Details:											
Authorization sources from which role mapping attributes are fetched (for each Authentication Source)											
		<table border="1"><thead><tr><th>Authentication Source</th><th>Attributes Fetched From</th></tr></thead><tbody><tr><td>1. [Guest User Repository] [Local SQL DB]</td><td>[Guest User Repository] [Local SQL DB]</td></tr><tr><td>2. AriyaAD [Active Directory]</td><td>AriyaAD [Active Directory]</td></tr></tbody></table>				Authentication Source	Attributes Fetched From	1. [Guest User Repository] [Local SQL DB]	[Guest User Repository] [Local SQL DB]	2. AriyaAD [Active Directory]	AriyaAD [Active Directory]
Authentication Source	Attributes Fetched From										
1. [Guest User Repository] [Local SQL DB]	[Guest User Repository] [Local SQL DB]										
2. AriyaAD [Active Directory]	AriyaAD [Active Directory]										
Additional authorization sources from which to fetch role-mapping attributes -											
		<div>[Endpoints Repository] [Local SQL DB] [Time Source] [Local SQL DB]</div> <div><div>Remove</div><div>View Details</div><div>Modify</div></div> <div>--Select to Add--</div>			Add new Authentication Source						

Summary	Service	Authentication	Authorization	Roles	Enforcement		
Role Mapping Policy: --Select-- <div>Modify</div> Add new Role Mapping Policy							
Role Mapping Policy Details							
Description:		-					
Default Role:		-					
Rules Evaluation Algorithm:		-					
<table border="1"><thead><tr><th>Conditions</th><th>Role</th></tr></thead><tbody></tbody></table>						Conditions	Role
Conditions	Role						

Summary	Service	Authentication	Authorization	Roles	Enforcement						
Use Cached Results: <input type="checkbox"/> Use cached Roles and Posture attributes from previous sessions											
Enforcement Policy: Ariya WiredAOS-S GuestEnforcement Policy <div>Modify</div> Add new Enforcement Policy											
Enforcement Policy Details											
Description:											
Default Profile:		[ArubaOS Switching - Bounce Switch Port]									
Rules Evaluation Algorithm:		first-applicable									
<table border="1"><thead><tr><th>Conditions</th><th>Enforcement Profiles</th></tr></thead><tbody><tr><td>1. (Tips:Role EQUALS [Guest])</td><td>Ariya AOS-S GuestMAC-Caching, Ariya AOS-S MAC Caching Expire Post Login, [Update Endpoint Known], [ArubaOS Switching - Bounce Switch Port]</td></tr><tr><td>2. (Authentication:Source EQUALS AriyaAD)</td><td>Ariya AOS-S AD-MAC-Caching, [ArubaOS Switching - Bounce Switch Port]</td></tr></tbody></table>						Conditions	Enforcement Profiles	1. (Tips:Role EQUALS [Guest])	Ariya AOS-S GuestMAC-Caching, Ariya AOS-S MAC Caching Expire Post Login, [Update Endpoint Known], [ArubaOS Switching - Bounce Switch Port]	2. (Authentication:Source EQUALS AriyaAD)	Ariya AOS-S AD-MAC-Caching, [ArubaOS Switching - Bounce Switch Port]
Conditions	Enforcement Profiles										
1. (Tips:Role EQUALS [Guest])	Ariya AOS-S GuestMAC-Caching, Ariya AOS-S MAC Caching Expire Post Login, [Update Endpoint Known], [ArubaOS Switching - Bounce Switch Port]										
2. (Authentication:Source EQUALS AriyaAD)	Ariya AOS-S AD-MAC-Caching, [ArubaOS Switching - Bounce Switch Port]										

6.8 Enforcement Profiles

Enforcement Profiles - Ariya AOS-S GuestMAC-Caching

Summary	Profile	Attributes
Profile:		
Name:	Ariya AOS-S GuestMAC-Caching	
Description:		
Type:	Post_Authentication	
Action:		
Device Group List:	-	
Attributes:		
Type	Name	Value
1. Endpoint	Username	= %{Authentication:Username}
2. Endpoint	Guest Role ID	= %{GuestUser:Role ID}
3. Endpoint	MAC-Auth Expiry	= %{Authorization:[Guest User Repository]:ExpireTime}

Now we need an enforcement profile for the AD users. Since captive portal-based access should only be temporary for employees, an expiration of one day will be used via [Time Source] which is a pre-built authentication source.

Enforcement Profiles - Ariya AOS-S AD-MAC-Caching

Summary	Profile	Attributes
Profile:		
Name:	Ariya AOS-S AD-MAC-Caching	
Description:		
Type:	Post_Authentication	
Action:		
Device Group List:	-	
Attributes:		
Type	Name	Value
1. Endpoint	Username	= %{Authentication:Username}
2. Endpoint	Guest Role ID	= AD-User
3. Endpoint	MAC-Auth Expiry	= %{Authorization:[Time Source]:One Day DT}

Since the above is a Post_Authentication profile, we'll write three attributes into the endpoint database.

1. the name of the user
2. the guest role ID which will be AD-User
3. and the expiry time which will be 1 day

Enforcement Profiles - Ariya WIRED-ArubaOS- MAC Caching Expire Post Login

Summary	Profile	Attributes
Profile:		
Name:	Ariya AOS-S MAC Caching Expire Post Login	
Description:		
Type:	Post_Authentication	
Action:		
Device Group List:	-	
Attributes:		
Type	Name	Value
1. Expire-Time-Update	GuestUser	= %{GuestUser:expire_postlogin}

Enforcement Profiles - WIRED-ArubaOS- MAC Caching Do Expire

Summary	Profile	Attributes
Profile:		
Name:	WIRED-ArubaOS- MAC Caching Do Expire	
Description:	Enforcement profile for User do expire functionality	
Type:	Post_Authentication	
Action:		
Device Group List:	-	
Attributes:		
Type	Name	Value
1. Expiry-Check	Expiry-Action	= %{GuestUser:do_expire}

Enforcement Profiles - [Update Endpoint Known]

Summary	Profile	Attributes
Profile:		
Name:	[Update Endpoint Known]	
Description:	System-defined profile to change Endpoint's status to Known	
Type:	Post_Authentication	
Action:		
Device Group List:	-	
Attributes:		
Type	Name	Value
1. Status-Update	Endpoint	= Known

Enforcement Profiles - [HPE Bounce Host-Port]

Summary	Profile	Attributes
Profile:		
Name:	[HPE Bounce Host-Port]	
Description:	System-defined profile to bounce host port (HPE)	
Type:	RADIUS_CoA	
Action:	CoA	
Device Group List:	-	
Attributes:		
Type	Name	Value
1. Radius:IETF	User-Name	= %{Radius:IETF:User-Name}
2. Radius:IETF	Calling-Station-Id	= %{Radius:IETF:Calling-Station-Id}
3. Radius:IETF	NAS-Port	= %{Radius:IETF:NAS-Port}
4. Radius:IETF	NAS-IP-Address	= %{Radius:IETF:NAS-IP-Address}
5. Radius:IETF	Event-Timestamp	=
6. Radius:Hewlett-Packard-Enterprise	HPE-Port-Bounce-Host	= 12

6.9 ClearPass Guest Splash Page

The enforcement profile that is used for captive portal redirection was "Ariya WIRED-ArubaOS- Guest Captive Portal" and the URL that it reference was https://192.168.1.94/guest/wired_guest.php

The only relevant settings on the guest side are the NAS Vendor Settings and the Login Delay.

Under NAS Vendor Settings, be sure the Vendor Settings are set to Hewlett Packard Enterprise. This will tell Guest to use a server-initiated login and which will craft a WEBAUTH request which is handled by the service we previously created.

Web Login Editor	
* Name:	<input type="text" value="wired-school"/> Enter a name for this web login page.
Page Name:	<input type="text" value="wired_guest"/> Enter a page name for this web login. The web login will be accessible from "/guest/page_name.php".
Description:	<div> <div></div> <div>Comments or descriptive text about the web login.</div> </div>
* Vendor Settings:	<div> <div>Hewlett Packard Enterprise</div> <div>▼</div> </div> Select a predefined group of settings suitable for standard network configurations.
Page Redirect Options for specifying parameters passed in the initial redirect.	
Security Hash:	<div> <div>Do not check – login will always be permitted</div> <div>▼</div> </div> Select the level of checking to apply to URL parameters passed to the web login page. Use this option to detect when URL parameters have been modified by the user, for example their MAC address.
Login Form Options for specifying the behaviour and content of the login form.	
Authentication:	<div> <div>Credentials – Require a username and password</div> <div>▼</div> </div> Select the authentication requirement. Access Code requires a single code (username) to be entered. Anonymous allows a blank form requiring just the terms or a Log In button. A pre-existing account is required. Auto is similar to anonymous but the page is automatically submitted. Access Code and Anonymous require the account to have the Username Authentication field set.
Prevent CNA:	<input checked="" type="checkbox"/> Enable bypassing the Apple Captive Network Assistant The Apple Captive Network Assistant (CNA) is the pop-up browser shown when joining a network that has a captive portal. Note that this option may not work with all vendors, depending on how the captive portal is implemented.
Custom Form:	<input type="checkbox"/> Provide a custom login form If selected, you must supply your own HTML login form in the Header or Footer HTML areas.
Custom Labels:	<input type="checkbox"/> Override the default labels and error messages If selected, you will be able to alter labels and error messages for the current login form.
* Pre-Auth Check:	<div> <div>None — no extra checks will be made</div> <div>▼</div> </div> Select how the username and password should be checked before proceeding to the NAS authentication.
Terms:	<input checked="" type="checkbox"/> Require a Terms and Conditions confirmation If checked, the user will be forced to accept a Terms and Conditions checkbox.
Default Destination Options for controlling the destination clients will redirect to after login.	
* Default URL:	<input type="text"/> Enter the default URL to redirect clients. Please ensure you prepend "http://" for any external domain.
Override Destination:	<input type="checkbox"/> Force default destination for all clients If selected, the client's default destination will be overridden regardless of its value.
Login Page Options for controlling the look and feel of the login page.	
* Skin:	<div> <div>Galleria Skin 2</div> <div>▼</div> </div> Choose the skin to use when this web login page is displayed.
Title:	<input type="text"/> The title to display on the web login page. Leave blank to use the default (Login).
Header HTML:	<div> <div> <pre>{nwa_cookiecheck} {if \$errmsg}{nwaicontext type=error}{\$errmsg escape}{/nwaicontext}{/if} {nwa_text id=7980}<p> Please login to the network using your username and password. </p>{/nwa_text}</pre> </div> <div>Insert... ▼</div> </div> HTML template code displayed before the login form.

Footer HTML:	<pre>{nwa_text id=7979}<p> Contact a staff member if you are experiencing difficulty logging in. </p>{/nwa_text}</pre> <div>Insert... ▼</div> <p>HTML template code displayed after the login form.</p>
Login Message:	<pre><p> Logging in, please wait... </p></pre> <div>Insert... ▼</div> <p>HTML template code displayed while the login attempt is in progress.</p>
* Login Delay:	<div>30 ▼</div> <p>The time in seconds to delay while displaying the login message.</p>

Advertising Services
[Enable advertising content on the login page.](#)

Advertising: ☐ Enable Advertising Services content

Cloud Identity
[Optionally present guests with various cloud identity / social login options.](#)

Enabled: ☐ Enable logins with cloud identity / social network credentials

Multi-Factor Authentication
[Require a secondary factor when authenticating.](#)

Provider:

No multi-factor authentication ▼

Network Login Access
[Controls access to the login page.](#)

Allowed Access:

Enter the IP addresses and networks from which logins are permitted.

Denied Access:

Enter the IP addresses and networks that are denied login access.

* Deny Behavior:

Send HTTP 404 Not Found status ▼

Select the response of the system to a request that is not permitted.

Post-Authentication
[Actions to perform after a successful pre-authentication.](#)

Health Check: ☐ Require a successful OnGuard health check
If selected, the guest will be required to pass a health check prior to accessing the network.

Update Endpoint: ☐ Mark the user's MAC address as a known endpoint
If selected, the endpoint's attributes will also be updated with other details from the user account.

Save Changes

Save and Reload

7 Testing Captive Portal with MAC Auth

Here we are testing the following scenario

1. new guest / temporary AD user connects to a switch port 4
 - a. there will be a MAC auth and CAPTIVE-PORTAL user role will be sent to the switch [the laptop is in VLAN 10]
 - b. the user's browser gets redirected to the captive portal page on ClearPass
 - c. the user enters the credential (cpguser) and click on the login button
 - d. the user will see 30sec delay countdown on the web page.
 - e. there will be a WEB-Auth and certain attributes gets written to the endpoint database
 - f. because we are using bounce switch port, after around 12 sec, the switch port will be bounced
 - g. there will be a MAC auth and this time based on the rules, a particular user-role will be sent to the switch

7.1 Guest User with Captive Portal with MAC Auth

Before we start let's have a look at configured user-roles.

```
Aruba-2930F-Lab2# sh user-role
```

User Roles

```
Enabled       : Yes
Initial Role  : denyall
```

Type	Name
local	Exec
local	GUEST
local	Staff
predefined	denyall
local	AD-Guest
local	Employee
local	Students
local	CORP-USER
local	MAC-AUTH-CORP
local	CAPTIVE-PORTAL

```
Aruba-2930F-Lab2#
```

```
Aruba-2930F-Lab2# sh port-access clients
```

Downloaded user roles are preceded by *

Port Access Client Status

Port	Client Name	MAC Address	IP Address	User Role	Type	VLAN
------	-------------	-------------	------------	-----------	------	------

```
Aruba-2930F-Lab2#
```

So now if we connect a non dot1x capable device to the same switch port, we see the MAC authentication happening along with Captive portal redirection. We are using the same laptop without enabling dot1x.

Summary	Input	Output	Accounting	Alerts
Login Status:	ACCEPT			
Session Identifier:	R00000004-01-5c3540ac			
Date and Time:	Jan 09, 2019 11:30:36 AEDT			
End-Host Identifier:	f0-de-f1-64-0a-82			
Username:	f0def1640a82			
Access Device IP/Port:	192.168.1.248:4 (Aruba-2930F-Lab2 / Hewlett-Packard-Enterprise)			
System Posture Status:	UNKNOWN (100)			
Policies Used -				
Service:	Ariya Wired-AOS-S MAC Auth			
Authentication Method:	MAC-AUTH			
Authentication Source:	None			
Authorization Source:	[Guest User Repository], [Guest Device Repository], [Endpoints Repository], [Insight Repository], [Time Source]			
Roles:	[Other], [User Authenticated]			
Enforcement Profiles:	Ariya Wired-AOS-S-Guest CaptivePortal			

Summary	Input	Output	Accounting	Alerts
Username:	f0def1640a82			
End-Host Identifier:	f0-de-f1-64-0a-82			
Access Device IP/Port:	192.168.1.248:4 (Aruba-2930F-Lab2 / Hewlett-Packard-Enterprise)			
RADIUS Request				
Authorization Attributes				
Computed Attributes				
Authentication:ErrorCode		0		
Authentication:Full-Username		f0def1640a82		
Authentication:Full-Username-Normalized		f0def1640a82		
Authentication:MacAuth		UnknownClient		
Authentication:OuterMethod		MAC-AUTH		
Authentication:Posture		Unknown		
Authentication:Status		MAB		
Authentication:Username		f0def1640a82		

Summary	Input	Output	Accounting	Alerts
Authorization:Sources	[Guest User Repository], [Guest Device Repository], [Endpoints Repository], [Insight Repository], [Time Source]			
Connection:Client-Mac-Address	f0-de-f1-64-0a-82			
Connection:Client-Mac-Address-Colon	f0:de:f1:64:0a:82			
Connection:Client-Mac-Address-Dot	f0de.f164.0a82			
Connection:Client-Mac-Address-Hyphen	f0-de-f1-64-0a-82			
Connection:Client-Mac-Address-NoDelim	f0def1640a82			
Connection:Client-Mac-Address-Upper-Hyphen	F0-DE-F1-64-0A-82			
Connection:Client-Mac-Vendor	Wistron Infocomm (Zhongshan) Corporation			
Connection:Dest-IP-Address	192.168.1.94			
Connection:Dest-Port	1812			
Connection:NAD-IP-Address	192.168.1.248			
Connection:Protocol	RADIUS			
Connection:Src-IP-Address	192.168.1.248			
Connection:Src-Port	1812			

Summary	Input	Output	Accounting	Alerts
Enforcement Profiles:	Ariya Wired-AOS-S-Guest CaptivePortal			
System Posture Status:	UNKNOWN (100)			
Audit Posture Status:	UNKNOWN (100)			
RADIUS Response				
Radius:Hewlett-Packard-Enterprise:HPE-Captive-Portal-URL	https://192.168.1.94/guest/wired_guest.php			
Radius:Hewlett-Packard-Enterprise:HPE-User-Role	CAPTIVE-PORTAL			
Radius:IETF:Session-Timeout	600			

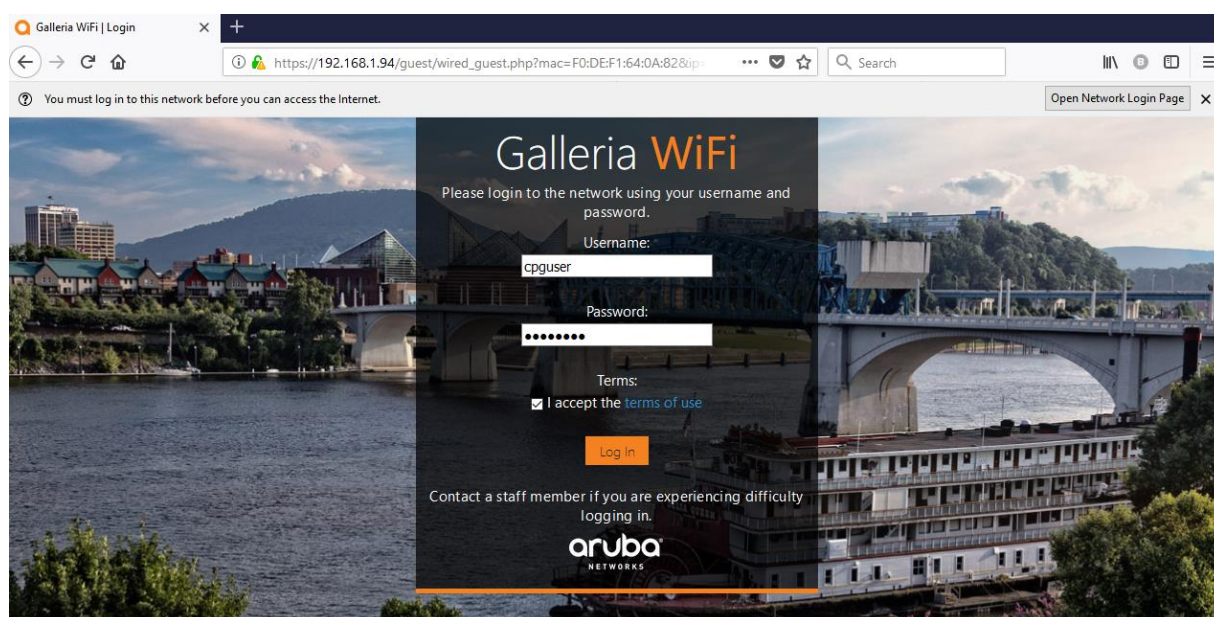
```
Aruba-2930F-Lab2# sh port-access client
Downloaded user roles are preceded by *
```

Port Access Client Status


Port	Client Name	MAC Address	IP Address	User Role	Type	VLAN
4	f0def1640a82	f0def1-640a82	10.10.10.100	CAPTIVE-PORTAL	MAC	10

```
Aruba-2930F-Lab2#
```

Now the guest user will start its web browser and in our example will browse to <http://airwave.mylab.com> gets redirected to Captive portal and uses "cpguser" guest account to login as shown below:



At this stage we should see a WEB-Auth session in ClearPass Access tracker.

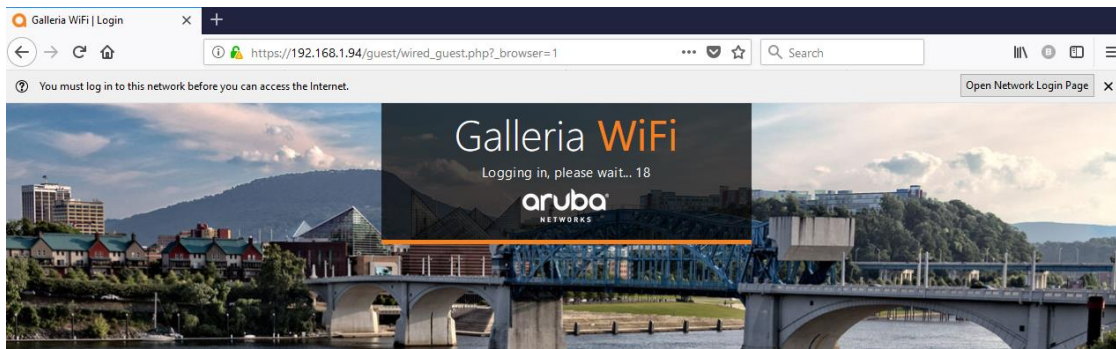
Summary	Input	Output
Login Status:		ACCEPT
Session Identifier:		W00000002-01-5c3541ad
Date and Time:		Jan 09, 2019 11:34:53 AEDT
End-Host Identifier:		f0def1640a82
Username:		cpguser
Access Device IP/Port:		-
System Posture Status:		UNKNOWN (100)
Policies Used -		
Service:		Ariya Wired-AOS-S GuestWebAuth 
Authentication Method:		Not applicable
Authentication Source:		[Guest User Repository]
Authorization Source:		[Guest User Repository], [Endpoints Repository], [Time Source]
Roles:		[Guest], [User Authenticated]
Enforcement Profiles:		Ariya AOS-S GuestMAC-Caching, Ariya AOS-S MAC Caching Expire Post Login, [Update Endpoint Known], [ArubaOS Switching - Bounce Switch Port]

Summary	Input	Output
Username:	cpguser	
End-Host Identifier:	f0def1640a82	
Access Device IP/Port:	-	
Authorization Attributes		
Computed Attributes		
Application:ClearPass:Page-Name	wired_guest	
Application:WebLoginURL:ip	10.10.10.100	
Application:WebLoginURL:mac	F0:DE:F1:64:0A:82	
Application:WebLoginURL:timestamp	1546993949	
Application:WebLoginURL:url	http://airwave.mylab.com/	
Authentication:Full-Username	cpguser	
Authentication:Full-Username-Normalized	cpguser	
Authentication:Posture	Unknown	
Authentication:Source	[Guest User Repository]	

Summary	Input	Output
Authentication:Status	User	
Authentication:Username	cpguser	
Authorization:Sources	[Guest User Repository], [Endpoints Repository], [Time Source]	
Connection:Client-IP-Address	10.10.10.100	
Connection:Client-Mac-Address	f0def1640a82	
Connection:Client-Mac-Address-Colon	f0:de:f1:64:0a:82	
Connection:Client-Mac-Address-Dot	f0de.f164.0a82	
Connection:Client-Mac-Address-Hyphen	f0-de-f1-64-0a-82	
Connection:Client-Mac-Address-NoDelim	f0def1640a82	
Connection:Client-Mac-Address-Upper-Hyphen	F0-DE-F1-64-0A-82	
Connection:Client-Mac-Vendor	Wistron Infocomm (Zhongshan) Corporation	
Connection:Protocol	WEBAUTH	
Connection:Src-IP-Address	127.0.0.1	
Date:Date-of-Year	2019-01-09	
Date:Date-Time	2019-01-09 11:24:52	

Summary	Input	Output
Enforcement Profiles:	Ariya AOS-S GuestMAC-Caching, Ariya AOS-S MAC Caching Expire Post Login, [Update Endpoint Known], [ArubaOS Switching - Bounce Switch Port]	
System Posture Status:	UNKNOWN (100)	
Audit Posture Status:	UNKNOWN (100)	
RADIUS Response		
Endpoint:Guest Role ID	2	
Endpoint:MAC-Auth Expiry	2019-03-30 16:32:45	
Endpoint:Username	cpguser	
Expire-Time-Update:GuestUser	0	
Radius:Hewlett-Packard-Enterprise:HPE-Port-Bounce-Host	12	
Radius:IETF:Calling-Station-Id	f0-de-f1-64-0a-82	
Radius:IETF:NAS-IP-Address	192.168.1.248	
Radius:IETF:NAS-Port	4	
Radius:IETF:User-Name	f0def1640a82	
Status-Update:Endpoint	Known	

The gest user will now see on the browser, the 30 sec countdown starts.



The endpoint database will be updated with guest expire time, username and status being known

Configuration » Identity » Endpoints

Endpoints

[Add](#)
[Import](#)
[Export All](#)

This page automatically lists all authenticated endpoints. An endpoint device is an Internet-capable hardware device on a TCP/IP network (e.g. laptops, smart phones, tablets, etc.).

Filter: contains [Go](#) [Clear Filter](#) Show records

#	MAC Address	Hostname	Device Category	Device OS Family	Status	Profiled
1.	<input type="checkbox"/> f0def1640a82		Computer	Windows	Known	Yes

Endpoint	Attributes	Device Fingerprints
MAC Address	f0def1640a82	IP Address10.10.10.100
Description		Static IPFALSE
Status	<div><div><div><div></div><div>Known client</div></div><div><div></div><div>Unknown client</div></div><div><div></div><div>Disabled client</div></div></div></div>	Hostname-
		Device CategoryComputer
		Device OS FamilyWindows
		Device NameWindows
MAC Vendor	Wistron Infocomm (Zhongshan) Corporation	Added AtJan 09, 2019 11:38:10 AEDT
Added by	Policy Manager	Last Profiled AtJan 09, 2019 11:38:10 AEDT
Online Status	Online	
Connection Type	Wired	
Switch IP	192.168.1.248	
Switch Port	4	
HPE_CompanyAsset	<div><div></div>Yes<div><div></div>No</div></div>	

Endpoint	Attributes	Device Fingerprints
Attribute	Value	
1. Guest Role ID	= 2	Copy Delete
2. MAC-Auth Expiry	= 2019-03-30 16:32:45	Copy Delete
3. Username	= cpguser	Copy Delete
4.	Click to add...	

There will be a port bounce and then we see a RADIUS MAC auth request come in with the correct username

Filter: contains [Go](#) [Clear Filter](#) Show records

#	Server	Source	Username	Service	Login Status	Request Timestamp
1.	192.168.1.94	RADIUS	cpguser	Ariya Wired-AOS-S MAC Auth	ACCEPT	2019/01/09 11:35:12
2.	192.168.1.94	WEBAUTH	cpguser	Ariya Wired-AOS-S GuestWebAuth	ACCEPT	2019/01/09 11:34:53
3.	192.168.1.94	RADIUS	f0def1640a82	Ariya Wired-AOS-S MAC Auth	ACCEPT	2019/01/09 11:33:35

Summary	Input	Output	Accounting
Login Status:	ACCEPT		
Session Identifier:	R00000006-01-5c3541c0		
Date and Time:	Jan 09, 2019 11:35:12 AEDT		
End-Host Identifier:	f0-de-f1-64-0a-82 (Computer / Windows / Windows)		
Username:	cpguser		
Access Device IP/Port:	192.168.1.248:4 (Aruba-2930F-Lab2 / Hewlett-Packard-Enterprise)		
System Posture Status:	UNKNOWN (100)		
Policies Used -			
Service:	Ariya Wired-AOS-S MAC Auth		
Authentication Method:	MAC-AUTH		
Authentication Source:	Local:localhost		
Authorization Source:	[Guest User Repository], [Guest Device Repository], [Endpoints Repository], [Insight Repository], [Time Source]		
Roles:	[Guest], [MAC Caching], [User Authenticated]		
Enforcement Profiles:	Ariya Wired-AOS-S-MAC-Auth Guest, Ariya Return-Endpoint-Username		

Summary	Input	Output	Accounting
Enforcement Profiles:	Ariya Wired-AOS-S-MAC-Auth Guest, Ariya Return-Endpoint-Username		
System Posture Status:	UNKNOWN (100)		
Audit Posture Status:	UNKNOWN (100)		
RADIUS Response			
Radius:Hewlett-Packard-Enterprise:HPE-User-Role	GUEST		
Radius:IETF:Session-Timeout	86400		
Radius:IETF:User-Name	cpguser		

And we see the user role changes to Guest.

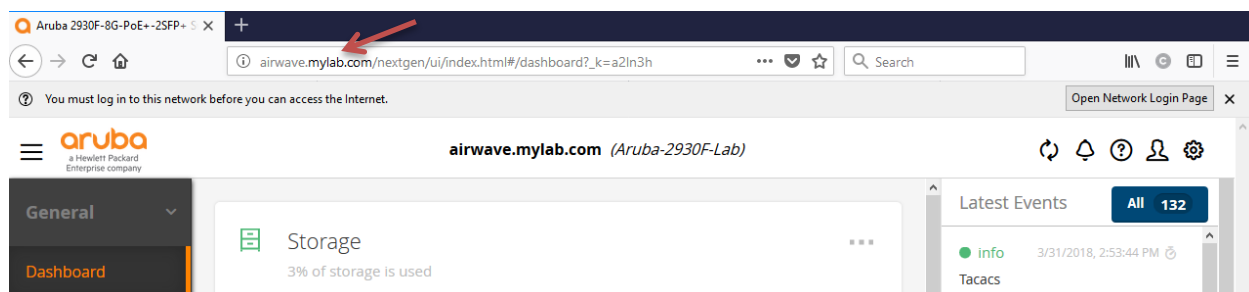
```
Aruba-2930F-Lab2# sh port-access client
```

Port Access Client Status

Port	Client Name	MAC Address	IP Address	User Role	Type	VLAN
4	cpguser	f0def1-640a82	10.10.10.100	GUEST	MAC	10

```
Aruba-2930F-Lab2#
```

Finally the user will be redirected to the original web page that they requested.



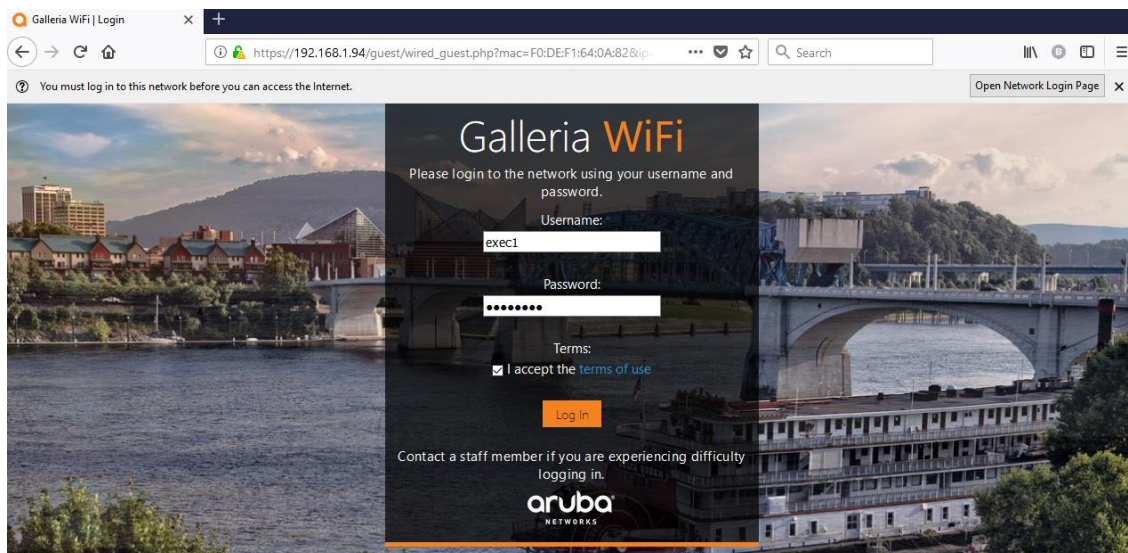
7.2 AD User with Captive Portal with MAC Auth

Now we'll test the temporary AD user using the captive portal to login. Since we are using the same laptop for this test, we'll delete its entry from the endpoint database and start new.

Here we'll use exec1 AD user. The workflow should be the same. The Captive Portal user role will be sent to the switch.

Summary	Input	Output	Accounting	Alerts
Login Status:	ACCEPT			
Session Identifier:	R00000009-01-5c354bb4			
Date and Time:	Jan 09, 2019 12:17:40 AEDT			
End-Host Identifier:	f0-de-f1-64-0a-82 (Computer / Windows / Windows)			
Username:	f0def1640a82			
Access Device IP/Port:	192.168.1.248:4 (Aruba-2930F-Lab2 / Hewlett-Packard-Enterprise)			
System Posture Status:	UNKNOWN (100)			
Policies Used -				
Service:	Ariya Wired-AOS-S MAC Auth			
Authentication Method:	MAC-AUTH			
Authentication Source:	None			
Authorization Source:	[Guest User Repository], [Guest Device Repository], [Endpoints Repository], [Insight Repository], [Time Source]			
Roles:	[Other], [User Authenticated]			
Enforcement Profiles:	Ariya Wired-AOS-S-Guest CaptivePortal			
Summary	Input	Output	Accounting	Alerts
Enforcement Profiles:	Ariya Wired-AOS-S-Guest CaptivePortal			
System Posture Status:	UNKNOWN (100)			
Audit Posture Status:	UNKNOWN (100)			
RADIUS Response				
Radius:Hewlett-Packard-Enterprise:HPE-Captive-Portal-URL	https://192.168.1.94/guest/wired_guest.php			
Radius:Hewlett-Packard-Enterprise:HPE-User-Role	CAPTIVE-PORTAL			
Radius:IETF:Session-Timeout	600			

The user uses exec1 credentials.



There will be a WEB-Auth request.

Summary	Input	Output	Alerts
Login Status:	ACCEPT		
Session Identifier:	W00000003-01-5c354c83		
Date and Time:	Jan 09, 2019 12:21:07 AEDT		
End-Host Identifier:	f0def1640a82		
Username:	exec1		
Access Device IP/Port:	-		
System Posture Status:	UNKNOWN (100)		
Policies Used -			
Service:	Ariya Wired-AOS-S GuestWebAuth		
Authentication Method:	Not applicable		
Authentication Source:	AriyaAD		
Authorization Source:	[Endpoints Repository], [Time Source], AriyaAD		
Roles:	[User Authenticated]		
Enforcement Profiles:	Ariya AOS-S AD-MAC-Caching, [ArubaOS Switching - Bounce Switch Port]		
Service Monitor Mode:	Disabled		

Summary	Input	Output	Alerts
Username:		exec1	
End-Host Identifier:		f0def1640a82	
Access Device IP/Port:		-	
Authorization Attributes			
Computed Attributes			
Application:ClearPass:Page-Name		wired_guest	
Application:WebLoginURL:ip		10.10.10.100	
Application:WebLoginURL:mac		F0:DE:F1:64:0A:82	
Application:WebLoginURL:timestamp		1546996651	
Application:WebLoginURL:url		http://airwave.mylab.com/	
Authentication:Full-Username		exec1	
Authentication:Full-Username-Normalized		exec1	
Authentication:Posture		Unknown	
Authentication:Source		AriyaAD	

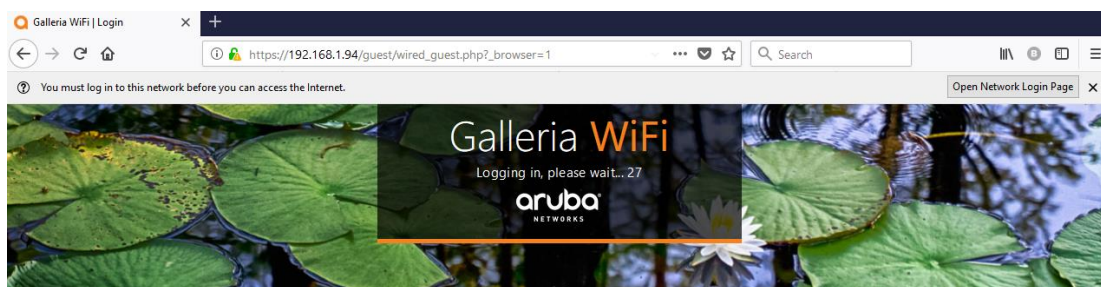
Summary	Input	Output	Alerts
Enforcement Profiles:	Ariya AOS-S AD-MAC-Caching, [ArubaOS Switching - Bounce Switch Port]		
System Posture Status:	UNKNOWN (100)		
Audit Posture Status:	UNKNOWN (100)		
RADIUS Response			
Endpoint:Guest Role ID	AD-User		
Endpoint:MAC-Auth Expiry	2019-01-10 12:00:00		
Endpoint:Username	exec1		
Radius:Hewlett-Packard-Enterprise:HPE-Port-Bounce-Host	12		
Radius:IETF:Calling-Station-Id	f0-de-f1-64-0a-82		
Radius:IETF:NAS-IP-Address	192.168.1.248		
Radius:IETF:NAS-Port	4		
Radius:IETF:User-Name	f0def1640a82		

Now the endpoint database entry will be slight different. Remember that for the AD user we are adding the guest role ID and expire time of one day.

Endpoint	Attributes	Device Fingerprints	Policy Cache
MAC Address	f0def1640a82	IP Address	10.10.10.100
Description		Static IP	FALSE
Status	<input type="radio"/> Known client <input checked="" type="radio"/> Unknown client <input type="radio"/> Disabled client	Hostname	-
MAC Vendor	Wistron Infocomm (Zhongshan) Corporation	Device Category	Computer
Added by	Policy Manager	Device OS Family	Windows
Online Status	<input checked="" type="checkbox"/> Online	Device Name	Windows
Connection Type	Wired	Added At	Jan 09, 2019 12:19:12 AEDT
Switch IP	192.168.1.248	Last Profiled At	Jan 09, 2019 12:19:12 AEDT
Switch Port	4		
HP_E_CompanyAsset	<input type="radio"/> Yes <input checked="" type="radio"/> No		

Endpoint	Attributes	Device Fingerprints	Policy Cache
Attribute	Value		
1. Guest Role ID	=	AD-User	
2. MAC-Auth Expiry	=	2019-01-10 12:00:00	
3. Username	=	exec1	
4. Click to add...			

There will be a port bounce.



The final MAC auth request comes in.

Filter:	Request ID	contains		Go	Clear Filter	Show 20 records
#	Server	Source	Username	Service	Login Status	Request Timestamp
1.	192.168.1.94	RADIUS	exec1	Ariya Wired-AOS-S MAC Auth	ACCEPT	2019/01/09 12:21:26
2.	192.168.1.94	WEBAUTH	exec1	Ariya Wired-AOS-S GuestWebAuth	ACCEPT	2019/01/09 12:21:07
3.	192.168.1.94	RADIUS	f0def1640a82	Ariya Wired-AOS-S MAC Auth	ACCEPT	2019/01/09 12:20:40

Summary	Input	Output	Accounting
Login Status:	ACCEPT		
Session Identifier:	R0000000b-01-5c354c96		
Date and Time:	Jan 09, 2019 12:21:26 AEDT		
End-Host Identifier:	f0-de-f1-64-0a-82 (Computer / Windows / Windows)		
Username:	exec1		
Access Device IP/Port:	192.168.1.248:4 (Aruba-2930F-Lab2 / Hewlett-Packard-Enterprise)		
System Posture Status:	UNKNOWN (100)		
Policies Used -			
Service:	Ariya Wired-AOS-S MAC Auth		
Authentication Method:	MAC-AUTH		
Authentication Source:	None		
Authorization Source:	[Guest User Repository], [Guest Device Repository], [Endpoints Repository], [Insight Repository], [Time Source]		
Roles:	[MAC Caching], [User Authenticated]		
Enforcement Profiles:	Ariya Wired-AOS-S-AD-Guest, Ariya Return-Endpoint-Username		

Summary	Input	Output	Accounting
Enforcement Profiles:	Ariya Wired-AOS-S-AD-Guest, Ariya Return-Endpoint-Username		
System Posture Status:	UNKNOWN (100)		
Audit Posture Status:	UNKNOWN (100)		
RADIUS Response			
Radius:Hewlett-Packard-Enterprise:HPE-User-Role	AD-Guest		
Radius:IETF:Session-Timeout	86400		
Radius:IETF:User-Name	exec1		

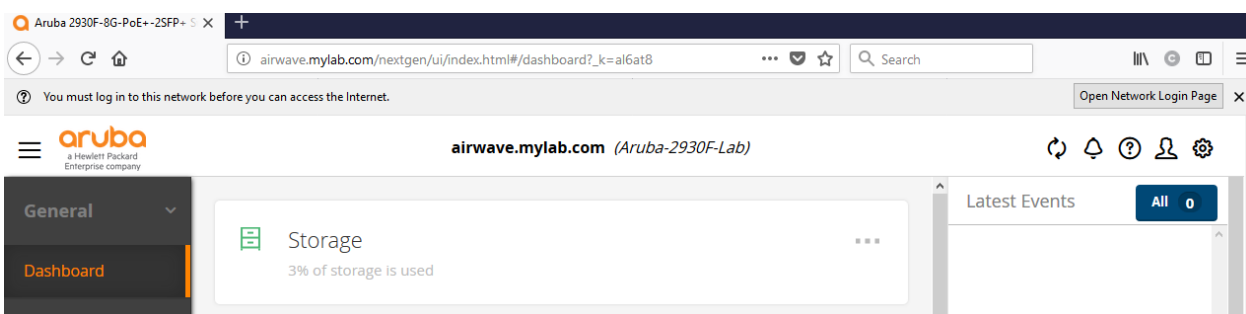
```
Aruba-2930F-Lab2# sh port-access client
```

Port Access Client Status

Port	Client Name	MAC Address	IP Address	User Role	Type	VLAN
4	exec1	f0def1-640a82	10.10.10.100	AD-Guest	MAC	10

```
Aruba-2930F-Lab2#
```

And the user gets redirected to the original URL before captive portal redirection.



In our demo the start URL was <http://airwave.mylab.com>

7.3 Aruba Switch Captive Portal Redirection

It should be noted that if the starting URL of the guest user while in Captive-Portal role is HTTPS, then the switch needs to have a HTTPS server certificate to be able to do the redirection, even a self-sign will do trick.

If you don't have this then the Captive portal redirection will not take place however HTTP will always work.

Here for our test, the initial URL in user's FF browser is <https://www.theage.com.au> as this is not a HSTS site, and FireFox will display Secure Connection failed. With the following message.

The page you are trying to view cannot be shown because the authenticity of the received data could not be verified.

Here we'll create a self-signed cert for this switch.

```
Aruba-2930F-Lab2# sh crypto pki local-certificate
```

Name	Usage	Expiration	Parent / Profile
IDEVID_CERT	IDEVID	2031/01/26	IDEVID_INTER_1
IDEVID_INTER_1	IDEVID	2031/01/26	IDEVID_INTER_2
IDEVID_INTER_2	IDEVID	2031/01/26	IDEVID_ROOT

```
Aruba-2930F-Lab2#
```

```
Aruba-2930F-Lab2(config)# crypto pki enroll-self-signed certificate-name DemoAriyaCert
key-type rsa key-size 1024 subject common-name
```

```
DemoAriya country AU locality Mel org Aruba org-unit IT state VIC usage captive-portal
```

```
Aruba-2930F-Lab2# sh crypto pki local-certificate
```

Name	Usage	Expiration	Parent / Profile
IDEVID_CERT	IDEVID	2031/01/26	IDEVID_INTER_1
IDEVID_INTER_1	IDEVID	2031/01/26	IDEVID_INTER_2
IDEVID_INTER_2	IDEVID	2031/01/26	IDEVID_ROOT
DemoAriyaCert	CaptivePortal	2019/04/03	default

```
Aruba-2930F-Lab2#
```

```
Aruba2930FDemo(config)#
```

Now you can check the self-signed certificate

```
Aruba-2930F-Lab2# sh crypto pki local-certificate DemoAriyaCert
```

Certificate Detail:

Version: 3 (0x2)

Serial Number:

50:3d:6a:a1:c1:a3:19:e7:30:9f:15:2d:d9:c8:63:ed:68:22:ce:17

Signature Algorithm: sha256withRSAEncryption

Issuer: CN=DemoAriya, OU=IT, O=Aruba, L=Mel, ST=VIC, C=AU

Validity

Not Before: Apr 3 11:34:02 2018 GMT

Not After : Apr 3 23:59:59 2019 GMT

Subject: CN=DemoAriya, OU=IT, O=Aruba, L=Mel, ST=VIC, C=AU

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public Key: (1024 bit)

Modulus (1024 bit):

30:0d:06:09:2a:86:48:86:f7:0d:01:01:01:05:00:
03:81:8d:00:30:81:89:02:81:81:00:d1:36:a1:ea:
d6:05:ac:52:19:f0:be:66:2f:6f:e4:a7:65:c6:e3:
de:99:9c:11:f1:2d:76:76:1b:42:43:0f:6e:bf:61:
c0:22:33:66:8d:64:6b:89:25:37:e7:ae:db:83:ed:
3d:92:ef:7f:72:97:c0:77:c7:5a:8f:f4:fa:f6:19:
f5:cb:75:00:8f:fe:68:ee:4f:1d:71:b5:75:7c:57:
7c:91:3b:0e:e1:1a:5b:01:55:a2:68:a1:35:83:84:
41:04:66:81:71:62:04:af:1f:77:57:5b:85:68:73:
f2:9e:d3:9e:84:75:25:8f:02:fe:39:f5:ef:c7:06:
67:e5:67:e3:02:03:01:00:01

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Key Usage: critical

Key Encipherment, Data Encipherment, Decipher Only

X509v3 Extended Key Usage:

TLS Web Server Authentication

Signature Algorithm: sha256withRSAEncryption

8a:f8:90:f9:82:e5:bf:63:3e:e8:af:d8:3a:fd:db:10:e4:da:
a2:ef:46:31:b9:b8:01:68:e0:48:03:04:32:61:01:ed:07:e3:
10:1c:e9:2b:63:34:52:12:84:f2:25:33:67:86:45:fb:3b:0a:
61:32:55:86:68:12:64:1c:29:7e:38:e4:5d:f5:dd:e4:1e:d4:
dc:c9:1a:ae:c5:f5:62:17:50:a7:ed:ed:de:a9:f5:ff:f2:16:
d9:fc:09:10:58:fd:38:86:93:d8:00:64:60:e7:01:ad:af:4e:
31:18:e5:fd:9f:73:2c:40:89:25:33:da:dc:11:3e:9b:b6:9d:
74:7e

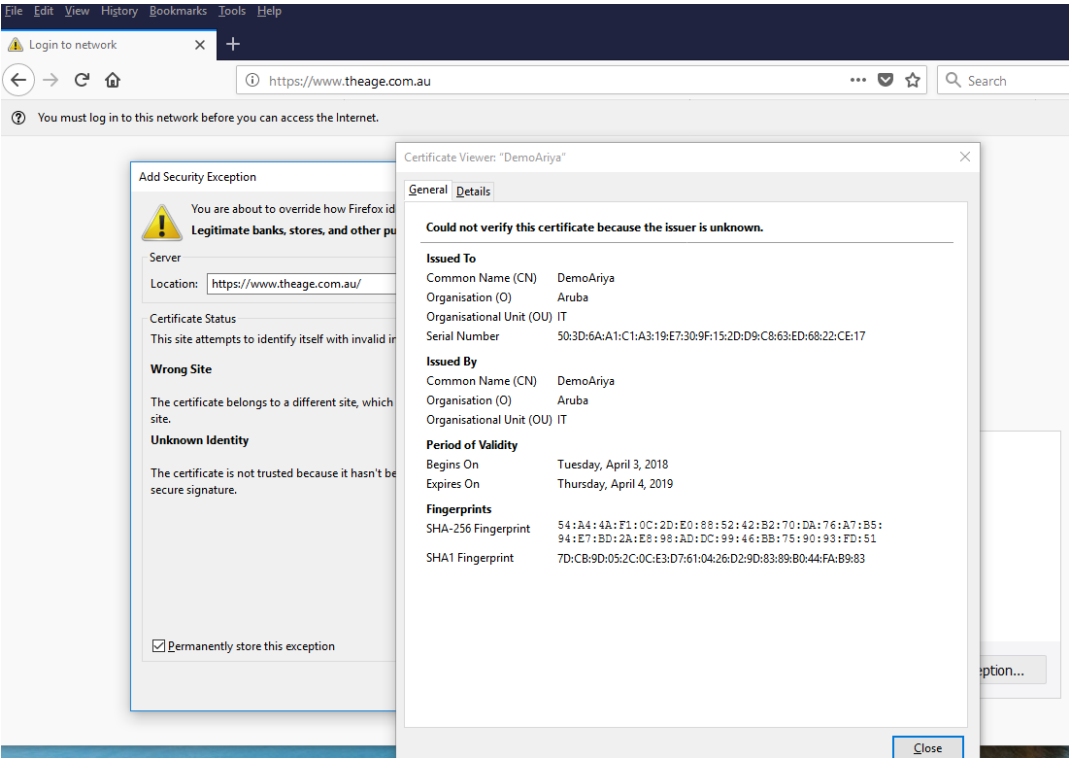
MD5 Fingerprint: f206 d3ae f6bd c910 9d69 aeb0 de3e c30e

SHA1 Fingerprint: 7dcb 9d05 2c0c e3d7 6104 26d2 9d83 89b0 44fa b983

```
Aruba-2930F-Lab2#
```


Now when the guest user browses to https://www.theage.com.au

The FF will display SEC-ERROR_UNKNOWN_ISSUER and now if you click on “Add Exception” and then click on the “View” certificate status you will see the newly created switch self-Signed cert



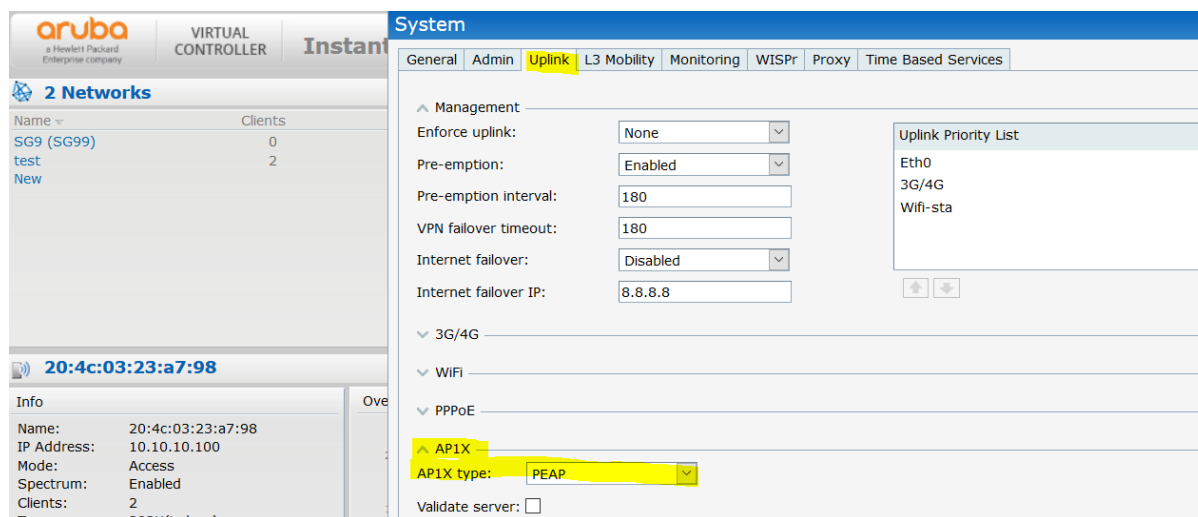
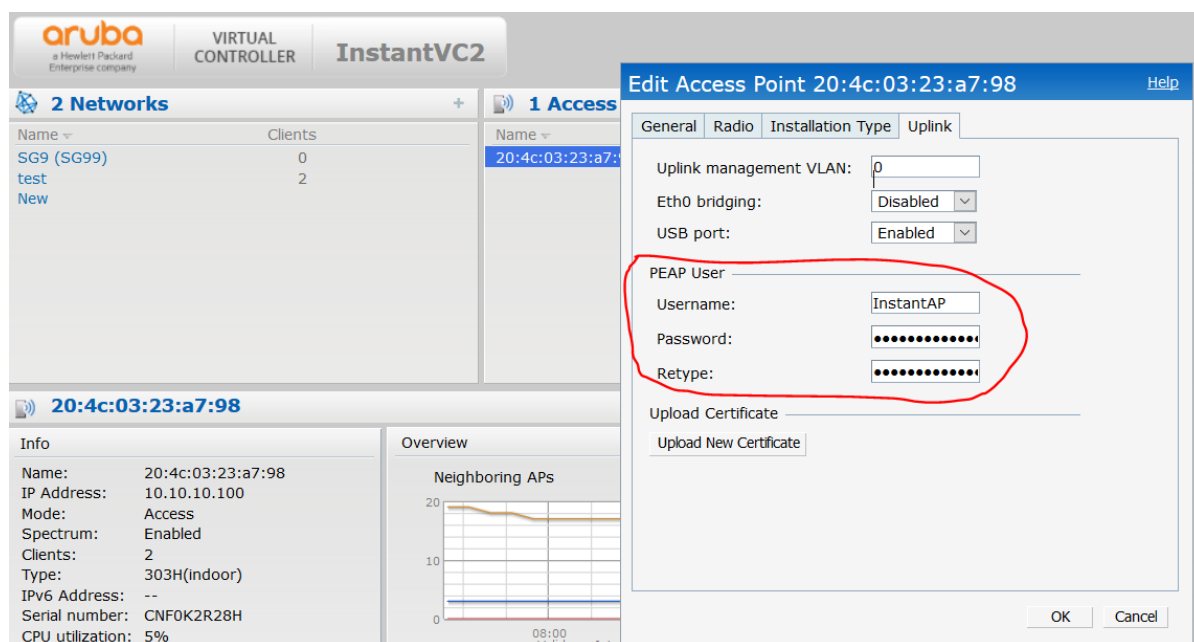
8 Wired Enforcement for Instant APs Dot1x

We are going to extend the concept of colourless port to the switch ports for Instant APs (IAP) as well.

The aim here is to do enable dot1x to authenticate the IAPs and then place the IAPs in their own user-roles with relevant untagged/tagged VLANs while allowing the wireless users connected to the IAPs to go through as per the authentication on the Wireless LAN configuration of the IAPs.

8.1 Instant AP Configuration

Here we enable the IAP for dot1x authentication. For simplicity we are going to use PEAP user InstantAP as the username



Once you have made the above changes, you need to reboot the IAP.

To verify the above configuration use these commands

```
20:4c:03:23:a7:98# sh ap1x config
#generated by rcS.fatap
ctrl_interface=/var/run/wpa_supplicant
ap_scan=0
eapol_version=1
fast_reauth=1
```

```

network={
  scan_ssid=0
  key_mgmt=IEEE8021X
  eap=PEAP
  eapol_flags=0
  identity="InstantAP"
  password="xxxxxxxx"
  phase1="crypto_binding=0"
  phase2="peaplabel=1"
  phase2="auth=MSCHAPV2"
  priority=1
}

```

20:4c:03:23:a7:98

8.2 Wired Dot1x Service Policy

We basically modify the previous wired dot1x service policy by adding a rule to the enforcement policy.

Services - Ariya WiredAOS-S Dot1x

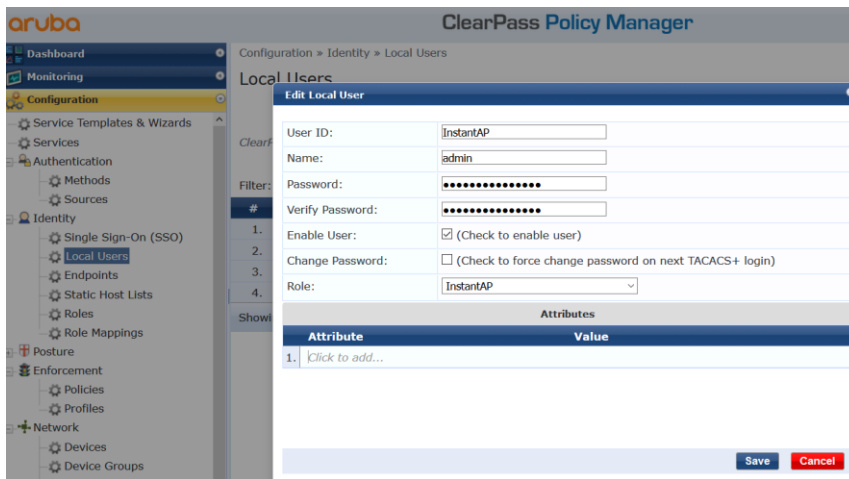
Summary	Service	Authentication	Roles	Enforcement
Use Cached Results:	<input type="checkbox"/> Use cached Roles and Posture attributes from previous sessions			
Enforcement Policy:	Ariya Wired-AOS-S Dot1xEnforcementPolicy Modify			Add New Enforcement Policy
Enforcement Policy Details				
Description:				
Default Profile:	[Deny Access Profile]			
Rules Evaluation Algorithm:	first-applicable			
Conditions		Enforcement Profiles		
1.	(Authorization:AriyaAD:memberOf CONTAINS staff)	Ariya Wired-AOS-S-Staff, [Update Endpoint Known]		
2.	(Authorization:AriyaAD:memberOf CONTAINS Stude)	Ariya Wired-AOS-S-Students, [Update Endpoint Known]		
3.	(Authorization:AriyaAD:memberOf CONTAINS exec)	Ariya DUR-Exec, Ariya HPE_Asset update, [Update Endpoint Known]		
4.	(Tips:Role EQUALS InstantAP)	Ariya Wired-AOS-S-IAP-1x		

Here is the enforcement profile.

Enforcement Profiles - Ariya Wired-AOS-S-IAP-1x

Summary	Profile	Attributes
Profile:		
Name:	Ariya Wired-AOS-S-IAP-1x	
Description:	InstantAP role	
Type:	RADIUS	
Action:	Accept	
Device Group List:	-	
Attributes:		
Type	Name	Value
1. Radius:Hewlett-Packard-Enterprise	HPE-User-Role	= InstantAP-1x

Finally you need to add the PEAP username that IAPs will use to the Local database of your ClearPass.



8.3 LAN Switch Configuration

Here we need to add the following configuration.

```
policy user "InstantAP"
  10 class ipv4 "HOME-LAN" action permit
  20 class ipv4 "INTERNET" action permit
  30 class ipv4 "IP-ANY-ANY" action permit
exit

aaa authorization user-role name "InstantAP-1x"
  policy "InstantAP"
  vlan-id 10
  vlan-id-tagged 20
  device
  port-mode
  exit
exit

aaa authorization user-role enable download
aaa authentication port-access eap-radius server-group "ClearPass"
aaa authentication mac-based chap-radius server-group "ClearPass"
aaa authentication captive-portal enable
aaa port-access authenticator 4
aaa port-access authenticator 4 tx-period 10
aaa port-access authenticator 4 supplicant-timeout 10
aaa port-access authenticator active
aaa port-access mac-based 4
aaa port-access 4 auth-order authenticator mac-based
aaa port-access 4 auth-priority authenticator mac-based
```

Using port-based mode, the first client authenticating on the port defines that access for all clients on that port. So if there are additional clients on the same port, they 'piggyback' on the access of the first device.

In our case, if we authenticate the access point, we don't want the switch to authenticate clients that are on the AP because the AP already authenticated them.

With this command "port-mode" ClearPass can change the switch port to port-based mode and allow all MAC addresses that are coming in over the access point skipping authentication for them.

The above aaa section was not changed and it is here for completeness.

8.4 Testing

Now is the time to test the setup which starts by the rebooting of the IAP.

```

APBoot 2.1.4.13 (build 59885)
Built: 2017-05-31 at 12:00:36

Model: AP-303H
DRAM: 512 MiB
Flash: Detected MX25L3205D: total 4 MiB
NAND: Detected MX35LFxGE4AB: total 128 MiB
Power: DC
Net: eth0
Radio: ipq4029#0, ipq4029#1
Reset: cold
FIPS: passed

Hit <Enter> to stop autoboot: 0
Booting OS partition 0
Checking image @ 0x0
Copying image from 0x84000000

Image is signed; verifying checksum... passed
SHA2 Signature available
Signer Cert OK
Policy Cert OK
< Deleted the whole bunch of output>
allow PAPI
set device anul0 mtu to 2000
notify asap_mod 3g no present...
Starting update SBL1 ...
SBL1 was updated already
Done.
trigger wpa_supplicant with configure file /aruba/aplx/wpa.conf
checking the authentication result and will time out at most 1 min
aplx authentication succeeded
Starting DHCP

```

And from the CLI of IAP you can also get the following

```

20:4c:03:23:a7:98# sh ap1x status

ap1x:peap
ap1x auth result:succeed
20:4c:03:23:a7:98#
20:4c:03:23:a7:98#
20:4c:03:23:a7:98# sh ap1x debug-logs
1970-01-01 00:00:38:apdot1x authentication type is peap
1970-01-01 00:00:38:trigger wpa_supplicant with configure file /aruba/aplx/wpa.conf
1970-01-01 00:00:38:checking the authenticaiton result and will time out at most 1 min
1970-01-01 00:00:53:ap1x authentication succeeded

20:4c:03:23:a7:98#

```

Now from ClearPass Access Tracker we get this.

#	Server	Source	Username	Service	Login Status	Request Timestamp ▾
1.	192.168.1.94	RADIUS	InstantAP	Ariya WiredAOS-S Dot1x	ACCEPT	2019/01/10 17:20:32
2.	192.168.1.94	RADIUS	204c0323a798	Ariya Wired-AOS-S MAC Auth	ACCEPT	2019/01/10 17:20:22

Summary	Input	Output	
Login Status:	ACCEPT		
Session Identifier:	R0000000f-01-5c382144		
Date and Time:	Jan 11, 2019 15:53:27 AEDT		
End-Host Identifier:	20-4c-03-23-a7-98 (Access Points / Aruba / Aruba IAP)		
Username:	InstantAP		
Access Device IP/Port:	192.168.1.248:4 (Aruba-2930F-Lab2 / Hewlett-Packard-Enterprise)		
System Posture Status:	UNKNOWN (100)		
Policies Used -			
Service:	Ariya WiredAOS-S Dot1x		
Authentication Method:	EAP-PEAP		
Authentication Source:	Local:localhost		
Authorization Source:	[Local User Repository]		
Roles:	InstantAP, [User Authenticated]		
Enforcement Profiles:	Ariya Wired-AOS-S-IAP-1x		
Service Monitor Mode:	Disabled		
Summary	Input	Output	Accounting
Username:	InstantAP		
End-Host Identifier:	20-4c-03-23-a7-98		
Access Device IP/Port:	192.168.1.248:4 (Aruba-2930F-Lab2 / Hewlett-Packard-Enterprise)		
RADIUS Request			
Computed Attributes			
Authentication:ErrorCode	0		
Authentication:Full-Username	InstantAP		
Authentication:Full-Username-Normalized	InstantAP		
Authentication:InnerMethod	EAP-MSCHAPv2		
Authentication:MacAuth	NotApplicable		
Authentication:OuterMethod	EAP-PEAP		
Authentication:Posture	Unknown		
Authentication:Source	[Local User Repository]		
Authentication:Status	User		
Summary	Input	Output	
Enforcement Profiles:	Ariya Wired-AOS-S-IAP-1x		
System Posture Status:	UNKNOWN (100)		
Audit Posture Status:	UNKNOWN (100)		
RADIUS Response			
Radius:Hewlett-Packard-Enterprise:HPE-User-Role InstantAP-1x			

And now from LAN switch CLI we see that

```
Aruba-2930F-Lab2# sh port-access clients
Downloaded user roles are preceded by *
```

Port Access Client Status

Port	Client Name	MAC Address	IP Address	User Role	Type	VLAN
4	InstantAP	204c03-23a798	n/a	InstantAP-1x	8021X	20, 10

```
Aruba-2930F-Lab2# sh port-access summary radius-overridden
```

Port Access Status Summary

```
Port-access authenticator activated [No] : Yes
Allow RADIUS-assigned dynamic (GVRP) VLANs [No] : No
```

```
Use LLDP data to authenticate [No] : No
Dot1X EAP Identifier Compliance [Disabled] : Disabled
```

Note: * indicates values dynamically overridden by RADIUS.

Port	Authenticator			Web Auth		MAC Auth			Local MAC	
	Enable	Mode	Limit	Enable	Limit	Enable	Mode	Limit	Enable	Limit
4	Yes	Port*	5	No	1	No*	User	5	No	1

```
Aruba-2930F-Lab2#
```

```
Aruba-2930F-Lab2# sh mac-address
```

Status and Counters - Port Address Table

MAC Address	Port	VLAN
204c03-23a798	4	10
b05ada-98b570	10	10
145f94-815626	10	192
204c03-23a7c0	10	192
483b38-724916	10	192

We also have a "Test" SSID that uses dot1x authentication configured on IAP that will get some clients to connect to.

2 Networks			1 Access Point			2 Clients on test			
Name	Clients		Name	Clients		Name	IP Address	ESSID	Access Point
SG9 (SG99)	0		20:4c:03:23:a7:98 *	2		staff1	10.10.10.102	test	20:4c:03:23:a7:98
test	2	edit x				student1	10.10.20.101	test	20:4c:03:23:a7:98
New									

As you can see we have 2x clients connected and each getting a different instant user-role and are put into different VLANs. (VLAN 10 and VLAN 20). From the LAN switch CLI we see there is still one user-role for port 4 however we see the new MAC address for these wireless clients in the MAC table.

```
Aruba-2930F-Lab2# sh port-access clients
```

Downloaded user roles are preceded by *

Port Access Client Status

Port	Client Name	MAC Address	IP Address	User Role	Type	VLAN
4	InstantAP	204c03-23a798	10.10.10.100	InstantAP-1x	8021X	20, 10

```
Aruba-2930F-Lab2# sh mac-address
```

Status and Counters - Port Address Table

MAC Address	Port	VLAN
204c03-23a798	4	10
a4d1d2-5f3252	4	10
b05ada-98b570	10	10
a088b4-50c084	4	20
b05ada-98b570	10	20
000c29-b82765	10	192
145f94-815626	10	192
204c03-23a7c0	10	192
483b38-724916	10	192

Now from the ClearPass access tracker we can verify that there is no additional request from the LAN switch. Note that we are also using the same ClearPass for wireless dot1x authentication.

#	Server	Source	Username	Service	Login Status	Request Timestamp ▾
1.	192.168.1.94	RADIUS	staff1	Lab Aruba 802.1X Wireless	ACCEPT	2019/01/10 17:30:56
2.	192.168.1.94	RADIUS	student1	Lab Aruba 802.1X Wireless	ACCEPT	2019/01/10 17:30:28
3.	192.168.1.94	RADIUS	InstantAP	Ariya WiredAOS-S Dot1x	ACCEPT	2019/01/10 17:20:32
4.	192.168.1.94	RADIUS	204c0323a798	Ariya Wired-AOS-S MAC Auth	ACCEPT	2019/01/10 17:20:22

9 Wired Enforcement for Instant APs MAC Auth

Here instead of using dot1x to authenticate the IAP we'll be using MAC Auth with ClearPass Profiling. Exactly same as last section except we'll be using ClearPass profiling mechanism.

9.1 Instant AP Configuration

Just ensure you have removed the AP1x setting and reboot the IAP.

The screenshot shows the Aruba InstantVC2 configuration interface. The 'Uplink' tab is selected under the 'System' section. The 'AP1X' section shows 'AP1X type' set to 'None'. The 'Uplink Priority List' shows 'Eth0', '3G/4G', and 'Wifi-sta'.

9.2 Wired MAC Auth Service Policy

We basically modify the previous Ariya Wired-AOS-S MAC Auth service by adding couple of rules to the enforcement policy

1. Since we have enabled profiling, we need to check for MAC spoofing and the first rule does that.
2. The last rule checks the endpoint repository and if the profiles info is Aruba Instant then we push IAP use role.

Summary	Service	Authentication	Authorization	Roles	Enforcement
Use Cached Results:	<input type="checkbox"/> Use cached Roles and Posture attributes from previous sessions				
Enforcement Policy:	<div>Ariya Wired-AOS-S MAC-Auth EnforcementPolicy Modify</div>				Add New Enforcement Policy
Enforcement Policy Details					
Description:					
Default Profile:	Ariya Wired-AOS-S-Guest CaptivePortal				
Rules Evaluation Algorithm:	first-applicable				
Conditions			Enforcement Profiles		
1.	(Authorization:[Endpoints Repository]:Conflict EXISTS)			Ariya Wired-AOS-S-MAC Spoof CaptivePortal	
2.	(Tips:Role EQUALS HPE_CompanyAsset)			Ariya Wired-AOS-S-CorpDevice	
3.	[User Authenticated] [Guest]]			Ariya Wired-AOS-S-MAC-Auth Guest, Ariya Return-Endpoint-Username	
4.	(Tips:Role EQUALS [MAC Caching]) AND (Endpoint:Guest Role ID EQUALS AD-User)			Ariya Wired-AOS-S-AD-Guest, Ariya Return-Endpoint-Username	
5.	(Authorization:[Endpoints Repository]:Device Name EQUALS Aruba IAP)			Ariya Wired-AOS-S-IAP	

Here are the enforcement profiles.

Enforcement Profiles - Ariya Wired-AOS-S-MAC Spoof CaptivePortal

Summary	Profile	Attributes	
Profile:			
Name:	Ariya Wired-AOS-S-MAC Spoof CaptivePortal		
Description:			
Type:	RADIUS		
Action:	Accept		
Device Group List:	-		
Attributes:			
	Type	Name	Value
1.	Radius:Hewlett-Packard-Enterprise	HPE-User-Role	= CAPTIVE-PORTAL
2.	Radius:Hewlett-Packard-Enterprise	HPE-Captive-Portal-URL	= https://192.168.1.94/guest/wired_mac_spoof.php
3.	Radius:IETF	Session-Timeout	= 600

Enforcement Profiles - Ariya Wired-AOS-S-IAP

Summary	Profile	Attributes
Profile:		
Name:	Ariya Wired-AOS-S-IAP	
Description:	InstantAP role	
Type:	RADIUS	
Action:	Accept	
Device Group List:	-	
Attributes:		
Type	Name	Value
1. Radius:Hewlett-Packard-Enterprise	HPE-User-Role	= InstantAP

9.3 LAN Switch Configuration

Here we need to add the following configuration.

```

policy user "InstantAP"
  10 class ipv4 "HOME-LAN" action permit
  20 class ipv4 "INTERNET" action permit
  30 class ipv4 "IP-ANY-ANY" action permit
exit

aaa authorization user-role name "InstantAP"
  policy "InstantAP"
  vlan-id 10
  vlan-id-tagged 20
  device
    port-mode
  exit
exit

vlan 10
  name "Lab-Mgmt-VLAN"
  ip address 10.10.10.2 255.255.255.0
  ip helper-address 192.168.1.94
exit

```

We have added the IP helper address so that ClearPass get to see the DHCP requests from the IAPs.

9.4 Testing

Now is the time to test the setup which starts by the rebooting of the IAP.

Now from ClearPass Access Tracker we get this.

Summary	Input	Output	Accounting
Login Status:	ACCEPT		
Session Identifier:	R00000010-01-5c3824ef		
Date and Time:	Jan 11, 2019 16:09:03 AEDT		
End-Host Identifier:	20-4c-03-23-a7-98 (Access Points / Aruba / Aruba IAP)		
Username:	204c0323a798		
Access Device IP/Port:	192.168.1.248:4 (Aruba-2930F-Lab2 / Hewlett-Packard-Enterprise)		
System Posture Status:	UNKNOWN (100)		
Policies Used -			
Service:	Ariya Wired-AOS-S MAC Auth		
Authentication Method:	MAC-AUTH		
Authentication Source:	None		
Authorization Source:	[Guest User Repository], [Guest Device Repository], [Endpoints Repository], [Insight Repository], [Time Source]		
Roles:	[Other], [User Authenticated]		
Enforcement Profiles:	Ariya Wired-AOS-S-IAP		

Summary	Input	Output	Accounting
Username:	204c0323a798		
End-Host Identifier:	20-4c-03-23-a7-98 (Access Points / Aruba / Aruba IAP)		
Access Device IP/Port:	192.168.1.248:4 (Aruba-2930F-Lab2 / Hewlett-Packard-Enterprise)		
RADIUS Request			
Authorization Attributes			
Computed Attributes			
Endpoint Attributes			
MAC Vendor	Aruba, a Hewlett Packard Enterprise Company		
Added by	Policy Manager		
Status	Unknown		
Device Category	Access Points		
Device OS Family	Aruba		
Device Name	Aruba IAP		
MAC Address	204c0323a798		
IP Address	10.10.10.100		

Summary	Input	Output	Accounting
Enforcement Profiles:	Ariya Wired-AOS-S-IAP		
System Posture Status:	UNKNOWN (100)		
Audit Posture Status:	UNKNOWN (100)		
RADIUS Response			
Radius:Hewlett-Packard-Enterprise:HPE-User-Role InstantAP			

And now from LAN switch CLI we see that

```
Aruba-2930F-Lab2# sh port-access clients
Downloaded user roles are preceded by *
```

Port Access Client Status

Port	Client Name	MAC Address	IP Address	User Role	Type	VLAN
4	InstantAP	204c03-23a798	n/a	InstantAP	8021X	20, 10

```
Aruba-2930F-Lab2# sh port-access summary radius-overridden
```

Port Access Status Summary

```

Port-access authenticator activated [No] : Yes
Allow RADIUS-assigned dynamic (GVRP) VLANs [No] : No
Use LLDP data to authenticate [No] : No
Dot1X EAP Identifier Compliance [Disabled] : Disabled

```

Note: * indicates values dynamically overridden by RADIUS.

Port	Authenticator			Web Auth		MAC Auth			Local MAC	
	Enable	Mode	Limit	Enable	Limit	Enable	Mode	Limit	Enable	Limit
4	Yes	User	5	No	1	Yes	Port* 5		No	1

```
Aruba-2930F-Lab2#
```

```
Aruba-2930F-Lab2# sh vlan port 4 det
```

Status and Counters - VLAN Information - for ports 4

VLAN ID	Name	Status	Voice	Jumbo	Mode
10	Lab-Mgmt-VLAN	Port-based	No	No	Untagged
20	Corp-VLAN	Port-based	No	No	Tagged

```
Aruba-2930F-Lab2#
```

We should also see the device information for the IAP under endpoints section of ClearPass

Configuration » Identity » Endpoints

Endpoints

[Add](#)
[Import](#)
[Export All](#)

This page automatically lists all authenticated endpoints. An endpoint device is an Internet-capable hardware device on a TCP/IP network (e.g. laptops, smart phones, tablets, etc.).

Filter: Device Category		contains	access	+	Go	Clear Filter	Show 20 records
#	MAC Address	Hostname	Device Category	Device OS Family	Status	Profiled	
1.	<input type="checkbox"/> 204c0323a798		Access Points	Aruba	Unknown	Yes	
Showing 1-1 of 1							
<div>Authentication Records</div> <div>Bulk Update</div> <div>Bulk Delete</div> <div>Trigger Server Action</div> <div>Update Fingerprint</div> <div>Export</div> <div>Delete</div>							

Endpoint	Attributes	Device Fingerprints
MAC Address	204c0323a798	IP Address 10.10.10.100
Description		Static IP FALSE
Status	<input type="radio"/> Known client <input checked="" type="radio"/> Unknown client <input type="radio"/> Disabled client	Hostname -
MAC Vendor	Aruba, a Hewlett Packard Enterprise Company	Device Category Access Points
Added by	Policy Manager	Device OS Family Aruba
Online Status	<input checked="" type="checkbox"/> Online	Device Name Aruba IAP
Connection Type	Wired	Added At Jan 11, 2019 14:29:49 AEDT
Switch IP	192.168.1.248	Last Profiled At Jan 11, 2019 16:09:31 AEDT
Switch Port	4	
HPE_CompanyAsset	<input type="radio"/> Yes <input checked="" type="radio"/> No	

Endpoint	Attributes	Device Fingerprints
Endpoint Fingerprint Details		
fingerprint.host.mac_vendor:	Aruba, a Hewlett Packard Enterprise Company	
DHCP Option60:	ArubaInstantAP	
DHCP Options:	53,61,60,50,54,55	
DHCP Option55:	1,3,4,6,12,15,28,42,43,60,66,67	

10 Wired Enforcement Critical Access

As more and more organisations will move to dynamic segmentation architecture that heavily relies on ClearPass, we should ensure that ClearPass is highly available. General recommendation is to have at least two node in a ClearPass cluster for redundancy.

In addition to this we have the concept of critical authentication user role feature on our LAN switches. It is the same concept as critical VLANs but for user roles.

Remember the original critical vlan was used when the authenticator server (ClearPass) was inaccessible, the switch can assign the interface to a VLAN that is defined critical VLAN. Normally, to avoid to impact service, critical VLAN is a normal VLAN that can access the appropriate resource. Here we have used the same concept but for user roles.

10.1 Aruba Switch Configuration

Here we have configured a new use role called Critical-role that gets reference from critical-auth

```
policy user "Critical"
  10 class ipv4 "HOME-LAN" action permit
  20 class ipv4 "INTERNET" action permit
  30 class ipv4 "IP-ANY-ANY" action permit
Exit

aaa authorization user-role name "Critical-role"
  policy "Critical"
  vlan-id 10
  vlan-id-tagged 20
  device
    port-mode
    exit
  exit

aaa port-access 4 critical-auth user-role "Critical-role"
```

Critical role is disabled by default. If the critical role is enabled and the client is unable to connect the switch and the RADIUS server, then the client moves to critical role. Any role can be configured as critical role.

10.2 Testing

Before we disconnect ClearPass from the network let's check the current status of the user-role for port4.

```
Aruba-2930F-Lab2# sh port-access clients
Downloaded user roles are preceded by *

Port Access Client Status

  Port  Client Name  MAC Address  IP Address  User Role  Type  VLAN
  ----  -
  4      InstantAP    204c03-23a798  10.10.10.100  InstantAP-1x  8021X  20, 10

Aruba-2930F-Lab2#

Aruba-2930F-Lab2# sh log -r
Keys:   W=Warning   I=Information
        M=Major    D=Debug   E=Error

---- Reverse event Log listing: Events Since Boot ----
```

```

I 01/11/19 17:02:48 00076 ports: port 4 is now on-line
I 01/11/19 17:02:48 00435 ports: port 4 is Blocked by AAA
I 01/11/19 17:02:48 00002 vlan: DEFAULT_VLAN virtual LAN disabled
I 01/11/19 17:02:48 00001 vlan: DEFAULT_VLAN virtual LAN enabled
I 01/11/19 17:02:29 00076 ports: port 4 is now on-line
I 01/11/19 17:02:22 00435 ports: port 4 is Blocked by AAA
I 01/11/19 17:02:18 00077 ports: port 4 is now off-line

```

So now if we disconnect ClearPass from the network and then disconnect and reconnect the IAP from the switch port.

```

Aruba-2930F-Lab2# sh port-access clients
Downloaded user roles are preceded by *

```

Port Access Client Status

Port	Client Name	MAC Address	IP Address	User Role	Type	VLAN
4		204c03-23a798	n/a		MAC	

```

Aruba-2930F-Lab2# sh port-access clients
Downloaded user roles are preceded by *

```

Port Access Client Status

Port	Client Name	MAC Address	IP Address	User Role	Type	VLAN
4		204c03-23a798	n/a		MAC	

```

Aruba-2930F-Lab2#

```

```

Aruba-2930F-Lab2# sh log -r

```

```

Keys:   W=Warning   I=Information
        M=Major     D=Debug   E=Error

```

```

---- Reverse event Log listing: Events Since Boot ----

```

```

I 01/11/19 17:12:50 00421 radius: Can't reach RADIUS server 192.168.1.94 (1
times in 60 seconds)
I 01/11/19 17:12:18 00427 802.1x: 2 auth-timeouts for the last 120 sec.
I 01/11/19 17:11:06 00421 radius: Can't reach RADIUS server 192.168.1.94 (2
times in 60 seconds)
I 01/11/19 17:10:18 00427 802.1x: 1 auth-timeouts for the last 60 sec.
I 01/11/19 17:10:14 00076 ports: port 4 is now on-line

```

```

Aruba-2930F-Lab2# sh port-access clients
Downloaded user roles are preceded by *

```

Port Access Client Status

Port	Client Name	MAC Address	IP Address	User Role	Type	VLAN
4		204c03-23a798	n/a		8021X	

```

Aruba-2930F-Lab2#

```

```

Aruba-2930F-Lab2#

```

```

Aruba-2930F-Lab2# sh port-access clients
Downloaded user roles are preceded by *

```

Port Access Client Status

Port	Client Name	MAC Address	IP Address	User Role	Type	VLAN
4		204c03-23a798	n/a		8021X	

```

Aruba-2930F-Lab2#

```

```

Aruba-2930F-Lab2# sh port-access clients

```

Downloaded user roles are preceded by *

Port Access Client Status

Port	Client Name	MAC Address	IP Address	User Role	Type	VLAN
4	InstantAP	204c03-23a798	10.10.10.100	Critical-role	8021X	20, 10

Aruba-2930F-Lab2#

And now when we connect back ClearPass we see

Aruba-2930F-Lab2# sh port-access clients

Downloaded user roles are preceded by *

Port Access Client Status

Port	Client Name	MAC Address	IP Address	User Role	Type	VLAN
4	InstantAP	204c03-23a798	10.10.10.100	InstantAP-1x	8021X	20, 10

Aruba-2930F-Lab2#

We'll see that the critical user role is now in play

11 Wired Enforcement for IP Phones

The aim here is to do a MAC Auth based on OUI for the Cisco IP Phones and then connect the Wired dot1x client at the back of an IP Phone and still get differentiated access based on the user type like staff or students. We need to create minimum of three services as shown below

8.	<input type="checkbox"/>	8	-----802.1X Wired Services-----	RADIUS	RADIUS Authorization	
9.	<input type="checkbox"/>	9	chisholm 802.1X Wired	RADIUS	802.1X Wired	
10.	<input type="checkbox"/>	10	Chisholm Wired MAC Auth and CP Redirection	RADIUS	MAC Authentication	
11.	<input type="checkbox"/>	11	Chisholm Wired Guest Web Login	WEBAUTH	Web-based Authentication	

11.1 Wired Dot1x Service Policy

This is the wired 802.1x policy that will differentiate between staff and students.

Summary	Service	Authentication	Authorization	Roles	Enforcement
Name: <input type="text" value="chisholm 802.1X Wired"/>					
Description: <input type="text" value="To authenticate users to any wired network via 802.1X."/>					
Type: <input type="text" value="802.1X Wired"/>					
Status: <input type="text" value="Enabled"/>					
Monitor Mode: <input type="checkbox"/> Enable to monitor network access without enforcement					
More Options: <input checked="" type="checkbox"/> Authorization <input type="checkbox"/> Posture Compliance <input type="checkbox"/> Audit End-hosts <input type="checkbox"/> Profile Endpoints <input type="checkbox"/> Accounting Proxy					
Service Rule					
Matches <input type="radio"/> ANY or <input checked="" type="radio"/> ALL of the following conditions:					
Type	Name	Operator	Value		
1. Radius:IETF	NAS-Port-Type	EQUALS	Ethernet (15)		
2. Radius:IETF	Service-Type	BELONGS_TO	Login-User (1), Framed-User (2), Authenticate-Only (8)		
3. Click to add...					

Summary	Service	Authentication	Authorization	Roles	Enforcement
Authentication Methods:					
<input type="text" value="[EAP PEAP]"/> <input type="text" value="[EAP TLS]"/> <input type="text" value="[EAP MSCHAPv2]"/>		<div><div>Move Up</div><div>Move Down</div><div>Remove</div><div>View Details</div><div>Modify</div></div>		Add new Authentication Method	
Authentication Sources:					
<input type="text" value="Chisholm-AD [Active Directory]"/> <input type="text" value="[Local User Repository] [Local SQL DB]"/>		<div><div>Move Up</div><div>Move Down</div><div>Remove</div><div>View Details</div><div>Modify</div></div>		Add new Authentication Source	
Strip Username Rules: <input type="checkbox"/> Enable to specify a comma-separated list of rules to strip username prefixes or suffixes					

Summary	Service	Authentication	Authorization	Roles	Enforcement
Authorization Details:					
Authorization sources from which role mapping attributes are fetched (for each Authentication Source)					
Authentication Source		Attributes Fetched From			
1.	Chisholm-AD [Active Directory]	Chisholm-AD [Active Directory]			
2.	[Local User Repository] [Local SQL DB]	[Local User Repository] [Local SQL DB]			
Additional authorization sources from which to fetch role-mapping attributes -					
<input type="text" value="Chisholm-AD [Active Directory]"/>		<div><div>Remove</div><div>View Details</div><div>Modify</div></div>		Add new Authentication Source	
<input type="text" value="--Select to Add--"/>					

Summary	Service	Authentication	Authorization	Roles	Enforcement
Role Mapping Policy: --Select-- Modify Add new Role Mapping Policy					
Role Mapping Policy Details					
Description:		-			
Default Role:		-			
Rules Evaluation Algorithm:		-			
Conditions			Role		

Summary	Service	Authentication	Authorization	Roles	Enforcement
Use Cached Results: <input type="checkbox"/> Use cached Roles and Posture attributes from previous sessions					
Enforcement Policy: chisholm 802.1X Wired Enforcement Policy Modify Add new Enforcement Policy					
Enforcement Policy Details					
Description:					
Default Profile:		[Deny Access Profile]			
Rules Evaluation Algorithm:		first-applicable			
Conditions			Enforcement Profiles		
1. (Authorization:Chisholm-AD:memberOf CONTAINS staff)			chisholm 802.1X Staff Wired		
2. (Authorization:Chisholm-AD:memberOf CONTAINS student)			chisholm 802.1X Student Wired		
3. (Tips:Role EQUALS Staff)			chisholm 802.1X Staff Wired		
4. (Tips:Role EQUALS Students)			chisholm 802.1X Student Wired		

This is the staff wired enforcement profile that we are using.

Enforcement Profiles - chisholm 802.1X Staff Wired

Summary	Profile	Attributes
Profile:		
Name:		chisholm 802.1X Staff Wired
Description:		Staff Wired
Type:		RADIUS
Action:		Accept
Device Group List:		-
Attributes:		
Type	Name	Value
1. Radius:Hewlett-Packard-Enterprise	HPE-User-Role	= StaffWired-3G

11.2 Wired MAC Auth with Captive Portal Service Policy

This is the policy to perform MAC auth of the IP Phones based on their OUI.

Summary	Service	Authentication	Roles	Enforcement
Name: Chisholm Wired MAC Auth and CP Redirection				
Description: MAC-based Authentication Service				
Type: MAC Authentication				
Status: Enabled				
Monitor Mode: <input type="checkbox"/> Enable to monitor network access without enforcement				
More Options: <input type="checkbox"/> Authorization <input type="checkbox"/> Audit End-hosts <input type="checkbox"/> Profile Endpoints <input type="checkbox"/> Accounting Proxy				
Service Rule				
Matches <input type="radio"/> ANY or <input checked="" type="radio"/> ALL of the following conditions:				
Type	Name	Operator	Value	
1. Radius:IETF	NAS-Port-Type	BELONGS_TO	Ethernet (15)	
2. Radius:IETF	Service-Type	BELONGS_TO	Login-User (1), Call-Check (10)	
3. Connection	Client-Mac-Address	EQUALS	%{Radius:IETF:User-Name}	
4. Radius:IETF	Connect-Info	CONTAINS	CONNECT	
5. Click to add...				

Summary	Service	Authentication	Roles	Enforcement
Authentication Methods: [Allow All MAC AUTH] Add new Authentication Method <div> Move Up Move Down Remove View Details Modify </div>				
Authentication Sources: [Endpoints Repository] [Local SQL DB] Add new Authentication Source <div> Move Up Move Down Remove View Details Modify </div>				
Strip Username Rules: <input type="checkbox"/> Enable to specify a comma-separated list of rules to strip username prefixes or suffixes				

This following is some of the Cisco IP Phone OUI and not the complete list.

Summary	Service	Authentication	Roles	Enforcement
Role Mapping Policy: Chisholm Role Mapping Modify Add new Role Mapping Policy				
Role Mapping Policy Details				
Description:				
Default Role: [Other]				
Rules Evaluation Algorithm: first-applicable				
Conditions			Role	
1.	(Radius:IETF:Calling-Station-Id CONTAINS 34-6f-90)		CISCO IPPhones	
2.	(Radius:IETF:Calling-Station-Id CONTAINS 00-17-5a)		CISCO IPPhones	
3.	(Radius:IETF:Calling-Station-Id CONTAINS 00:a3:d1)		CISCO IPPhones	
Summary			Enforcement	
Use Cached Results: <input checked="" type="checkbox"/> Use cached Roles and Posture attributes from previous sessions				
Enforcement Policy: Chisholm Wired MAC Auth and Redirection Modify Add new Enforcement Policy				
Enforcement Policy Details				
Description:				
Default Profile: CHI Wired Captive-Portal				
Rules Evaluation Algorithm: first-applicable				
Conditions			Enforcement Profiles	
1.	(Tips:Role EQUALS [Guest]) (Tips:Role EQUALS [User Authenticated]) AND (Authorization:[Endpoints Repository]:Status EQUALS Known)		CHI Wired Guest, CHI return-endpoint-username	
2.	(Tips:Role EQUALS CISCO IPPhones)		chisholm IP Phones	
3.	(Tips:Role EQUALS Corporate PCs)		chisholm 802.1X Staff Wired	

And here is the IP Phone enforcement Profile that we are using.

Summary	Profile	Attributes
Profile:		
Name:	chisholm IP Phones	
Description:	Chisholm IP Phones	
Type:	RADIUS	
Action:	Accept	
Device Group List:	-	
Attributes:		
Type	Name	Value
1. Radius:Hewlett-Packard-Enterprise	HPE-User-Role	= MAC-AUTH-IPPhone-3G

Here we have connected the IP Phone to port 1/16 and at the back of it we have connected a laptop that does dot1x and upon successful dot1x authentication it should be put into the Wired Staff VLAN. You can use the following debug commands to get a better insight into the RADIUS authentication on Aruba Switches. The IP address 10.65.33.66 is the ClearPass Server.

```
Aruba-Stack-2930M-1# debug security radius-server
Aruba-Stack-2930M-1# debug destination session

Aruba-Stack-2930M-1#
0003:21:30:57.92 RAD mRadiusCtrl:Received RADIUS MSG: AUTH REQUEST, session:
195, access method: PORT-ACCESS.
```

```

0003:21:30:57.92 RAD mRadiusCtrl:Received RADIUS MSG: DATA, session: 195.
0003:21:30:57.92 RAD mRadiusCtrl:ACCESS REQUEST id: 5 to 10.65.33.66 session:
195, access method: PORT-ACCESS, User-Name: staff, Calling-Station-Id:
f0def1-640a82, NAS-Port-Id: 1/16, NAS-IP-Address: 10.73.91.254.
0003:21:30:58.32 RAD tRadiusR:ACCESS CHALLENGE id: 5 from 10.65.33.66 received.
0003:21:30:58.32 RAD mRadiusCtrl:Received RADIUS MSG: DATA, session: 195.
0003:21:30:58.32 RAD mRadiusCtrl:ACCESS REQUEST id: 6 to 10.65.33.66 session:
195, access method: PORT-ACCESS, User-Name: staff, Calling-Station-Id:
f0def1-640a82, NAS-Port-Id: 1/16, NAS-IP-Address: 10.73.91.254.
0003:21:30:58.36 RAD tRadiusR:ACCESS CHALLENGE id: 6 from 10.65.33.66 received.
0003:21:30:58.37 RAD mRadiusCtrl:Received RADIUS MSG: DATA, session: 195.
0003:21:30:58.41 RAD mRadiusCtrl:ACCESS REQUEST id: 8 to 10.65.33.66 session:
195, access method: PORT-ACCESS, User-Name: staff, Calling-Station-Id:
f0def1-640a82, NAS-Port-Id: 1/16, NAS-IP-Address: 10.73.91.254.

```

So once the user gets successfully authenticated they are put into the Staff VLAN.


```
Aruba-Stack-2930M-1# sh port-access clients
```

Port Access Client Status

Port	Client Name	MAC Address	IP Address	User Role	Type	VLAN
1/16	staff	f0def1-640a82	10.73.70.8	StaffWired-3G	8021X	1100
1/16	346f9017ab52	346f90-17ab52	10.73.90.13	MAC-AUTH-IPPho...	MAC	

```
Aruba-Stack-2930M-1#
```

Here is the view of the access tracker

Summary	Input	Output	Accounting
Login Status:	ACCEPT		
Session Identifier:	R0000133d-01-59dc21e4		
Date and Time:	Oct 10, 2017 12:27:05 AEDT		
End-Host Identifier:	f0-de-f1-64-0a-82 (Computer / Windows / Windows)		
Username:	staff		
Access Device IP/Port:	10.73.91.254:16 (ArubaSwitch73 / Hewlett-Packard-Enterprise)		
System Posture Status:	UNKNOWN (100)		
Policies Used -			
Service:	chisholm 802.1X Wired		
Authentication Method:	EAP-PEAP,EAP-MSCHAPv2		
Authentication Source:	Local:localhost		
Authorization Source:	[Local User Repository], Chisholm-AD		
Roles:	Staff, [User Authenticated]		
Enforcement Profiles:	chisholm 802.1X Staff Wired		
Service Monitor Mode:	Disabled		
Online Status:	 Online		

Summary	Input	Output	Accounting
Username:	staff		
End-Host Identifier:	f0-de-f1-64-0a-82 (Computer / Windows / Windows)		
Access Device IP/Port:	10.73.91.254:16 (ArubaSwitch73 / Hewlett-Packard-Enterprise)		
RADIUS Request			
Authorization Attributes			
Computed Attributes			
Authentication:ErrorCode	0		
Authentication:Full-Username	staff		
Authentication:Full-Username-Normalized	staff		
Authentication:InnerMethod	EAP-MSCHAPv2		
Authentication:MacAuth	NotApplicable		
Authentication:OuterMethod	EAP-PEAP		
Authentication:Posture	Unknown		
Authentication:Source	[Local User Repository]		
Authentication:Status	User		
Authentication:Username	staff		
Authorization:Source	[Local User Repository], Chisholm-AD		

Summary	Input	Output	Accounting			
Enforcement Profiles:	chisholm 802.1X Staff Wired					
System Posture Status:	UNKNOWN (100)					
Audit Posture Status:	UNKNOWN (100)					
RADIUS Response						
Radius:Hewlett-Packard-Enterprise:HPE-User-Role StaffWired-3G						

12 Downloadable User Roles

Downloadable user roles (DUR) is a new feature on Aruba switches. This allows ClearPass to be the centralised policy point and send all the user roles and its related policies to the LAN switch. This means we don't have to configure the user-roles, and its policies in the LAN switches. In this example we have an AD group called Executives and want to put the users in this group on their own VLAN (20) and apply some traffic policies.

12.1 ClearPass Service Configuration

First we need to create a DUR enforcement profile. Note that when you create a new enforcement profile choose the type "Aruba Downloadable Role Enforcement".

Configuration » Enforcement » Profiles » Add Enforcement Profile

Enforcement Profiles

Profile	Attributes	Summary
Template:	Aruba Downloadable Role Enforcement	
Name:	Ariya DUR-Staff	
Description:		
Type:	RADIUS	
Action:	<input checked="" type="radio"/> Accept <input type="radio"/> Reject <input type="radio"/> Drop	
Device Group List:	<div>--Select--</div> <div>Remove View Details Modify</div>	
Role Configuration Mode:	<input type="radio"/> Standard <input checked="" type="radio"/> Advanced	
Product:	ArubaOS-Switch	

Here we are using the advance mode.

Summary	Profile	Attributes
Profile:		
Name:	Ariya DUR-Staff	
Description:		
Type:	RADIUS	
Action:	Accept	
Device Group List:	-	
Product:	ArubaOS-Switch	
Attributes:		
Type	Name	Value
1.	Radius:Hewlett-Packard-Enterprise	HPE-CPPM-Role
class ipv4 HOME-LAN match ip 0.0.0.0 255.255.255.255 192.168.1.0 0.0.0.255 exit class ipv4 INTERNET match ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 exit class ipv4 IP-ANY-ANY match ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 exit policy user Staff class ipv4 "HOME-LAN" action permit class ipv4 "INTERNET" action permit class ipv4 "IP-ANY-ANY" action permit exit aaa authorization user-role name Staff policy "Staff" vlan-id 10 exit		

Also you need to use "radius:Hewlett-Packard-Enterprise" rather than "Radius:Aruba"

```
class ipv4 HOME-LAN
match ip 0.0.0.0 255.255.255.255 192.168.1.0 0.0.0.255
```

```

exit

class ipv4 INTERNET
match ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
exit

class ipv4 IP-ANY-ANY
match ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
exit

policy user Staff
class ipv4 "HOME-LAN" action permit
class ipv4 "INTERNET" action permit
class ipv4 "IP-ANY-ANY" action permit
exit

aaa authorization user-role name Staff
policy "Staff"
vlan-id 10
exit

```

Similarly we'll create DUR for Students except we'll put them in to vlan 20.

Summary	Profile	Attributes		
Profile:				
Name:	Ariya DUR-Student			
Description:				
Type:	RADIUS			
Action:	Accept			
Device Group List:	-			
Product:	ArubaOS-Switch			
Attributes:				
Type	Name	Value		
1.	Radius:Hewlett-Packard-Enterprise	HPE-CPPM-Role	=	class ipv4 HOME-LAN match ip 0.0.0.0 255.255.255.255 192.168.1.0 0.0.0.255 exit
				class ipv4 INTERNET match ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 exit
				class ipv4 IP-ANY-ANY match ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 exit
				policy user Students class ipv4 "HOME-LAN" action permit class ipv4 "INTERNET" action permit class ipv4 "IP-ANY-ANY" action permit exit
				aaa authorization user-role name Students policy "Staff" vlan-id 20 exit

Now we need to change the enforcement policy in our existing dot1x service to reflect this. Here is the enforcement tab of the service we created in the earlier section, and we have now added the second condition.

Summary	Service	Authentication	Roles	Enforcement
Use Cached Results:	<input type="checkbox"/> Use cached Roles and Posture attributes from previous sessions			
Enforcement Policy:	<div><div>Ariya Wired-AOS-S Dot1xEnforcementPolicy</div><div>Modify</div></div>			Add New Enforcement Policy
Enforcement Policy Details				
Description:				
Default Profile:	[Deny Access Profile]			
Rules Evaluation Algorithm:	first-applicable			
Conditions		Enforcement Profiles		
1.	(Authorization:AriyaAD:memberOf CONTAINS staff)	Ariya DUR-Staff, [Update Endpoint Known]		
2.	(Authorization:AriyaAD:memberOf CONTAINS Stude)	Ariya DUR-Student, [Update Endpoint Known]		
3.	(Authorization:AriyaAD:memberOf CONTAINS exec)	Ariya DUR-Exec, Ariya HPE_Asset update, [Update Endpoint Known]		
4.	(Tips:Role EQUALS InstantAP)	Ariya Wired-AOS-S-IAP-1x		

12.2 Aruba Switch Configuration

DURs also require a ClearPass read-only user account to download the user role configuration. Here we configure the expected username and password for the account.

```
radius-server cppm identity aoss-DUR key aruba123
aaa authorization user-role enable download
```

Some legacy secure client access functionality is not supported when user roles are enabled.

CPPM user name and password must be configured for downloading the user role.
 CPPM HTTPS root certificate must be installed for downloading the user role.

```
Aruba-2930F-Lab2(config)#
```

And its corresponding account on ClearPass side.

Administration » Users and Privileges » Admin Users

Filter:	User ID	contains		Go	Clear Filter	Show 10 records
#	<input type="checkbox"/> User ID ▲	Name	Privilege Level	Status		
1.	<input type="checkbox"/> admin	Super Admin	Super Administrator	Enabled		
2.	<input type="checkbox"/> aoss-DUR	DUR user	Read-only Administrator	Enabled		
3.	<input type="checkbox"/> apiadmin	API Admin	API Administrator	Enabled		
Showing 1-3 of 3					Export	Delete

Lastly DUR will not work if your ClearPass has a self-signed HTTPS server certificate. You need to have a proper public server certificate.

Here I am using poc.clearpass.info server certificate signed by StartCom CA and hence we need to add StartCom Server CA in PEM format to the switch.

Server Certificates

Service Certificates

Select Server:

poc.clearpass.info

Select Type:

HTTPS Server Certificate

Subject:	CN=poc.clearpass.info, C=AU
Issued by:	CN=StartCom Class 1 DV Server CA, OU=StartCom Certification Authority, O=StartCom Ltd., C=IL
Issue Date:	Dec 14, 2016 18:21:22 AEDT
Expiry Date:	Dec 14, 2019 18:21:22 AEDT
Validity Status:	Valid
Details:	View Details

Intermediate CA Certificate:

Subject:	CN=StartCom Class 1 DV Server CA, OU=StartCom Certification Authority, O=StartCom Ltd., C=IL
Issued by:	CN=StartCom Certification Authority, OU=Secure Digital Certificate Signing, O=StartCom Ltd., C=IL
Issue Date:	Dec 16, 2015 12:00:05 AEDT
Expiry Date:	Dec 16, 2030 12:00:05 AEDT
Validity Status:	Valid
Details:	View Details

Root CA Certificate:

Subject:	CN=StartCom Certification Authority, OU=Secure Digital Certificate Signing, O=StartCom Ltd., C=IL
Issued by:	CN=StartCom Certification Authority, OU=Secure Digital Certificate Signing, O=StartCom Ltd., C=IL

Once you have root CA trusted cert file in PEM format, you can either tftp it to the switch or use the legacy Web UI.

12.3 Automatic Certificate download with ClearPass

With AOS-S 16.08, the switch has the ability to automatically download the root CA certificate of ClearPass servers.

First we list the current TA profiles on the switch.

```
Aruba-2930F-Lab2# sh crypto pki ta-profile
```

Profile Name	Profile Status	CRL Configured	OCSP Configured
IDEVID_ROOT	Root Certificate Installed		
COMODO_CA	Root Certificate Installed	No	No
Default	Root Certificate Installed	No	No
GEOTRUST_CA	Root Certificate Installed	No	No
ARUBA_CA	Root Certificate Installed	No	No
ADDTRUST_CA	Root Certificate Installed	No	No

```
Aruba-2930F-Lab2#
```

So instead of importing it manually, now you can automatically download it by adding “clearpass” to the end of the following command.

```
Aruba-2930F-Lab2(config)# radius-server host 192.168.1.94 key "aruba123" clearpass
Aruba-2930F-Lab2#
Aruba-2930F-Lab2# sh log -r
Keys:    W=Warning    I=Information
        M=Major      D=Debug    E=Error
---- Reverse event Log listing: Events Since Boot ----
I 01/21/19 10:57:28 05811 CADownload: Successfully downloaded the certificate
from 192.168.1.94 server
I 01/21/19 10:57:11 05101 amp-server: AMP server configuration is disabled due
to first configuration.
I 01/21/19 10:51:46 00179 mgr: SME SSH from 192.168.1.134 - MANAGER Mode
I 01/21/19 10:51:45 03362 auth: User 'unknown' logged in from 192.168.1.134 to
```

Checking the TA list again

```
Aruba-2930F-Lab2# sh crypto pki ta-profile
```

Profile Name	Profile Status	CRL Configured	OCSP Configured
IDEVID_ROOT	Root Certificate Installed		
COMODO_CA	Root Certificate Installed	No	No
Default	Root Certificate Installed	No	No
GEOTRUST_CA	Root Certificate Installed	No	No

ARUBA_CA	Root Certificate Installed	No	No
ADDTRUST_CA	Root Certificate Installed	No	No
StartCom Cer...	Root Certificate Installed	No	No

So expanding it we see

```
Aruba-2930F-Lab2# sh crypto pki ta-profile "StartCom Certification Authority"
Profile Name      Profile Status      CRL Configured      OCSP Configured
-----
StartCom Certification Authority 1 certificate installed      No      No

Trust Anchor:
Version: 3 (0x2)
Serial Number: 1 (0x1)
Signature Algorithm: sha1withRSAEncryption
Issuer: C=IL, O=StartCom Ltd., OU=Secure Digital Certificate Signing, CN=StartCom Certification Authority
Validity
  Not Before: Sep 17 19:46:36 2006 GMT
  Not After : Sep 17 19:46:36 2036 GMT
Subject: C=IL, O=StartCom Ltd., OU=Secure Digital Certificate Signing, CN=StartCom Certification Authority
Subject Public Key Info:
  Public Key Algorithm: rsaEncryption
  RSA Public Key: (4096 bit)
    Modulus (4096 bit):
      30:0d:06:09:2a:86:48:86:f7:0d:01:01:01:05:00:
      03:82:02:0f:00:30:82:02:0a:02:82:02:01:00:c1:
      88:db:09:bc:6c:46:7c:78:9f:95:7b:b5:33:90:f2:
      72:62:d6:c1:36:20:22:24:5e:ce:e9:77:f2:43:0a:
      a2:06:64:a4:cc:8e:36:f8:38:e6:23:f0:6e:6d:b1:
      3c:dd:72:a3:85:1c:a1:d3:3d:b4:33:2b:d3:2f:af:
      fe:ea:b0:41:59:67:b6:c4:06:7d:0a:9e:74:85:d6:
      79:4c:80:37:7a:df:39:05:52:59:f7:f4:1b:46:43:
      a4:d2:85:85:d2:c3:71:f3:75:62:34:ba:2c:8a:7f:
      1e:8f:ee:ed:34:d0:11:c7:96:cd:52:3d:ba:33:d6:
      dd:4d:de:0b:3b:4a:4b:9f:c2:26:2f:fa:b5:16:1c:
      72:35:77:ca:3c:5d:e6:ca:e1:26:8b:1a:36:76:5c:
      01:db:74:14:25:fe:ed:b5:a0:88:0f:dd:78:ca:2d:
      1f:07:97:30:01:2d:72:79:fa:46:d6:13:2a:a8:b9:
      a6:ab:83:49:1d:e5:f2:ef:dd:e4:01:8e:18:0a:8f:
      63:53:16:85:62:a9:0e:19:3a:cc:b5:66:a6:c2:6b:
      74:07:e4:2b:e1:76:3e:b4:6d:d8:f6:44:e1:73:62:
      1f:3b:c4:be:a0:53:56:25:6c:51:09:f7:aa:ab:ca:
      bf:76:fd:6d:9b:f3:9d:db:bf:3d:66:bc:0c:56:aa:
      af:98:48:95:3a:4b:df:a7:58:50:d9:38:75:a9:5b:
      ea:43:0c:02:ff:99:eb:e8:6c:4d:70:5b:29:65:9c:
      dd:aa:5d:cc:af:01:31:ec:0c:eb:d2:8d:e8:ea:9c:
      7b:e6:6e:f7:27:66:0c:1a:48:d7:6e:42:e3:3f:de:
      21:3e:7b:e1:0d:70:fb:63:aa:a8:6c:1a:54:b4:5c:
      25:7a:c9:a2:c9:8b:16:a6:bb:2c:7e:17:5e:05:4d:
      58:6e:12:1d:01:ee:12:10:0d:c6:32:7f:18:ff:fc:
      f4:fa:cd:6e:91:e8:36:49:be:1a:48:69:8b:c2:96:
      4d:1a:12:b2:69:17:c1:0a:90:d6:fa:79:22:48:bf:
      ba:7b:69:f8:70:c7:fa:7a:37:d8:d8:0d:d2:76:4f:
      57:ff:90:b7:e3:91:d2:dd:ef:c2:60:b7:67:3a:dd:
      fe:aa:9c:f0:d4:8b:7f:72:22:ce:c6:9f:97:b6:f8:
      af:8a:a0:10:a8:d9:fb:18:c6:b6:b5:5c:52:3c:89:
      b6:19:2a:73:01:0a:0f:03:b3:12:60:f2:7a:2f:81:
      db:a3:6e:ff:26:30:97:f5:8b:dd:89:57:b6:ad:3d:
      b3:af:2b:c5:b7:76:02:f0:a5:d6:2b:9a:86:14:2a:
      72:f6:e3:33:8c:5d:09:4b:13:df:bb:8c:74:13:52:
      4b:02:03:01:00:01
    Exponent: 65537 (0x10001)
X509v3 extensions:
  X509v3 Basic Constraints:
    CA:TRUE
  X509v3 Key Usage:
    Key Encipherment, Data Enchipherment, Decipher Only
  X509v3 Subject Key Identifier:
```

4e:0b:ef:1a:a4:40:5b:a5:17:69:87:30:ca:34:68:43:d0:41:ae:f2

X509v3 CRL Distribution Points:

URI: http://cert.startcom.org/sfsca-crl.crl

URI: http://crl.startcom.org/sfsca-crl.crl

X509v3 Certificate Policies:

Policy:0.1.4.1.23223.1.1.1.48.257.59.48.47.6.8.43.6.1.5.5.7.2.1.22.35.104.116.116.112.58.47.47.99.101.114.116.46.115.116.97.114.116.99.111.109.46.111.114.103.47.112.111.108.105.99.121.46.112.100.102.48.53.6.8.43.6.1.5.5.7.2.1.22.41.104.116.116.112.58.47.47.99.101.114.116.46.115.116.97.114.116.99.111.109.46.111.114.103.47.105.110.116.101.114.109.101.100.105.97.116.101.46.112.100.102.48.26630.8.43.6.1.5.5.7.2.2.48.25008.39.22.32.83.116.97.114.116.32.67.111.109.109.101.114.99.105.97.108.32.40.83.116.97.114.116.67.111.109.41.32.76.116.100.46.48.3.2.1.1.26.19404.105.109.105.116.101.100.32.76.105.97.98.105.108.105.116.121.44.32.114.101.97.100.32.116.104.101.32.115.101.99.116.105.111.110.32.42.76.101.103.97.108.32.76.105.109.105.116.97.116.105.111.110.115.42.32.111.102.32.116.104.101.32.83.116.97.114.116.67.111.109.32.67.101.114.116.105.102.105.99.97.116.105.111.110.32.65.117.116.104.111.114.105.116.121.32.80.111.108.105.99.121.32.97.118.97.105.108.97.98.108.101.32.97.116.32.104.116.116.112.58.47.47.99.101.114.116.46.115.116.97.114.116.99.111.109.46.111.114.103.47.112.111.108.105.99.121

Users associated with this TA profile

Aruba-2930F-Lab2#

12.4 DUR Testing

When the staff1 user connects to the LAN switch port 4 there is a MAC auth and then dot1x request and we see this in ClearPass access tracker.

Filter:	<div>Request ID</div>	<div>contains</div>	<div></div>	<div>+</div>	<div>Go</div>	<div>Clear Filter</div>	Show <div>20</div> records
#	Server	Source	Username	Service	Login Status	Request Timestamp ▾	
1.	192.168.1.94	RADIUS	staff1	Ariya WiredAOS-S Dot1x	ACCEPT	2019/01/13 13:40:33	
2.	192.168.1.94	RADIUS	f0def1640a82	Ariya Wired-AOS-S MAC Auth-DUR	ACCEPT	2019/01/13 13:40:17	

Summary	Input	Output	Accounting
Login Status:	ACCEPT		
Session Identifier:	R00000002-01-5c3aa521		
Date and Time:	Jan 13, 2019 13:40:33 AEDT		
End-Host Identifier:	f0-de-f1-64-0a-82 (Computer / Windows / Windows)		
Username:	staff1		
Access Device IP/Port:	192.168.1.248:4 (Aruba-2930F-Lab2 / Hewlett-Packard-Enterprise)		
System Posture Status:	UNKNOWN (100)		
Policies Used -			
Service:	Ariya WiredAOS-S Dot1x		
Authentication Method:	EAP-PEAP,EAP-MSCHAPv2		
Authentication Source:	AD:192.168.1.250		
Authorization Source:	AriyaAD		
Roles:	[User Authenticated]		
Enforcement Profiles:	[Update Endpoint Known], Ariya DUR-Staff		
Service Monitor Mode:	Disabled		

Summary	Input	Output	Accounting
Enforcement Profiles:	[Update Endpoint Known], Ariya DUR-Staff		
System Posture Status:	UNKNOWN (100)		
Audit Posture Status:	UNKNOWN (100)		
RADIUS Response			
Radius:Hewlett-Packard-Enterprise:HPE-CPPM-Role		Ariya_DUR_Staff-3035-2 class ipv4 HOME-LAN match ip 0.0.0.0 255.255.255.255 192.168.1.0 0.0.0.255 exit class ipv4 INTERNET match ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 exit class ipv4 IP-ANY-ANY match ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 exit	

And we here is the output of relevant commands for verification.

```
Aruba-2930F-Lab2# sh port-access clients
```

Downloaded user roles are preceded by *

Port Access Client Status

Port	Client Name	MAC Address	IP Address	User Role	Type	VLAN
4	staff1	f0def1-640a82	10.10.10.101	*Ariya_DUR_Sta...	8021X	10

```
Aruba-2930F-Lab2#
```

```
Aruba-2930F-Lab2# sh user-role
```

Downloaded user roles are preceded by *

User Roles

```
Enabled      : Yes
Initial Role : denyall
```

Type	Name
local	Exec
local	GUEST
local	Staff
predefined	denyall
local	AD-Guest
local	Employee
local	Students
local	CORP-USER
local	MAC-AUTH-CORP
local	CAPTIVE-PORTAL
downloaded	*Ariya_DUR_Exec-3035-2

```
Aruba-2930F-Lab2#
```

```
Aruba-2930F-Lab2# show port-access clients detailed
```

Port Access Client Status Detail

Client Base Details :

```

Port          : 4
Client Status : authenticated
Client name   : staff1
MAC Address   : f0def1-640a82
IP            : 10.10.10.101

Authentication Type : 802.1x
Session Time       : 1191 seconds
Session Timeout    : 0 seconds

```

```
Auth Order      : Mac-Auth, 8021x
Auth Priority    : 8021x, Mac-Auth
LMA Fallback     : Disabled
```

Downloaded user roles are preceded by *

User Role Information

```
Name                : *Ariya_DUR_Staff-3035-2
Type                : downloaded
Reauthentication Period (seconds) : 0
Cached Reauth Period (seconds)    : 0
Logoff Period (seconds)           : 300
Untagged VLAN          : 10
Tagged VLANs           :
Captive Portal Profile :
Policy                 : Staff_Ariya_DUR_Staff-3035-2
```

Statements for policy "Staff_Ariya_DUR_Staff-3035-2"

policy user "Staff_Ariya_DUR_Staff-3035-2"

```
10 class ipv4 "HOME-LAN_Ariya_DUR_Staff-3035-2" action permit
20 class ipv4 "INTERNET_Ariya_DUR_Staff-3035-2" action permit
30 class ipv4 "IP-ANY-ANY_Ariya_DUR_Staff-3035-2" action permit
exit
```

Statements for class IPv4 "HOME-LAN_Ariya_DUR_Staff-3035-2"

class ipv4 "HOME-LAN_Ariya_DUR_Staff-3035-2"

```
10 match ip 0.0.0.0 255.255.255.255 192.168.1.0 0.0.0.255
exit
```

Statements for class IPv4 "INTERNET_Ariya_DUR_Staff-3035-2"

class ipv4 "INTERNET_Ariya_DUR_Staff-3035-2"

```
10 match ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
exit
```

Statements for class IPv4 "IP-ANY-ANY_Ariya_DUR_Staff-3035-2"

class ipv4 "IP-ANY-ANY_Ariya_DUR_Staff-3035-2"

```
10 match ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
exit
```

```
Tunnelednode Server Redirect : Disabled
Secondary Role Name          :
Device Attributes             : Disabled
```

Aruba-2930F-Lab2#

12.5 DUR with Captive Portal

When using DUR you can't refer to the captive-portal profile defined on the switch. You need to use DUR for that as well. Here we create another two advance DUR enforcement profile in ClearPass.

Enforcement Profiles - Ariya DUR-Guest-CP

Summary

Profile

Attributes

Profile:

Name:	Ariya DUR-Guest-CP
Description:	
Type:	RADIUS
Action:	Accept
Device Group List:	-
Product:	ArubaOS-Switch

Attributes:

Type	Name	Value
1.	Radius:Hewlett-Packard-Enterprise	<div>class ipv4 DUR-DHCP</div> <div>10 match udp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 67</div> <div>exit</div>
		<div>class ipv4 DUR-IP-ANY-ANY</div> <div>10 match ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255</div> <div>exit</div>
		<div>class ipv4 DUR-WEB-TRAFFIC</div> <div>10 match tcp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 80</div> <div>20 match tcp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 443</div> <div>exit</div>
		<div>class ipv4 DUR-DNS-INTERNAL</div> <div>10 match udp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 53</div> <div>exit</div>
		<div>class ipv4 DUR-CLEARPASS-WEB</div> <div>10 match tcp 0.0.0.0 255.255.255.255 192.168.1.94 0.0.0.0 eq 80</div> <div>20 match tcp 0.0.0.0 255.255.255.255 192.168.1.94 0.0.0.0 eq 443</div> <div>exit</div>
	HPE-CPPM-Role	=

Here is the details of the attribute value

```

class ipv4 DUR-DHCP
10 match udp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 67
exit

class ipv4 DUR-IP-ANY-ANY
10 match ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
exit

class ipv4 DUR-WEB-TRAFFIC
10 match tcp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 80
20 match tcp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 443
exit

class ipv4 DUR-DNS-INTERNAL
10 match udp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 53
exit

class ipv4 DUR-CLEARPASS-WEB
10 match tcp 0.0.0.0 255.255.255.255 192.168.1.94 0.0.0.0 eq 80
20 match tcp 0.0.0.0 255.255.255.255 192.168.1.94 0.0.0.0 eq 443
exit

aaa authentication captive-portal profile CP-Portal url
https://192.168.1.94/guest/wired guest.php

policy user DUR-CLEARPASS-REDIRECT
10 class ipv4 DUR-DNS-INTERNAL action permit
20 class ipv4 DUR-DHCP action permit
30 class ipv4 DUR-CLEARPASS-WEB action permit
40 class ipv4 DUR-WEB-TRAFFIC action redirect captive-portal
50 class ipv4 DUR-IP-ANY-ANY action deny
exit

aaa authorization user-role name Quarantine
policy DUR-CLEARPASS-REDIRECT
captive-portal-profile CP-Portal
vlan-id 10
exit

```

The second enforcement profile for successful MAC-auth

Summary	Profile	Attributes		
Name:	Ariya DUR-MAC-Auth			
Description:				
Type:	RADIUS			
Action:	Accept			
Device Group List:	-			
Product:	ArubaOS-Switch			
Attributes:				
Type	Name	Value		
1.	Radius:Hewlett-Packard-Enterprise	HPE-CPPM-Role	=	class ipv4 DUR-Guest-DHCP
				10 match udp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 67
				exit
				class ipv4 DUR-Guest-DNS
				10 match udp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 53
				exit
				class ipv4 DUR-Internal-Net
				10 match ip 0.0.0.0 255.255.255.255 10.10.30.0 0.0.0.255
				exit
				class ipv4 DUR-Internet
				10 match ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
				exit
				policy user DUR-Guest
				10 class ipv4 DUR-Guest-DHCP action permit
				20 class ipv4 DUR-Guest-DNS action permit
				30 class ipv4 DUR-Internal-Net action deny
				40 class ipv4 DUR-Internet action permit
				exit
				aaa authorization user-role name DUR-Guest
				reauth-period 3600

Here is the details of the attribute value

```
class ipv4 DUR-Guest-DHCP
    10 match udp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 67
    exit
class ipv4 DUR-Guest-DNS
    10 match udp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 53
    exit
class ipv4 DUR-Internal-Net
    10 match ip 0.0.0.0 255.255.255.255 10.10.30.0 0.0.0.255
    exit
class ipv4 DUR-Internet
    10 match ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
    exit

policy user DUR-Guest
    10 class ipv4 DUR-Guest-DHCP action permit
    20 class ipv4 DUR-Guest-DNS action permit
    30 class ipv4 DUR-Internal-Net action deny
    40 class ipv4 DUR-Internet action permit
    exit









aaa authorization user-role name DUR-Guest
    reauth-period 3600
    vlan-id 10
    policy DUR-Guest
    exit
```

Now we can either modify our default enforcement profile in the policy we used in “Ariya Wired-AOS-S MAC Auth” service, or create a new service. Here we have chosen to create a new service so we can easily enable/disable them.

7.	<input type="checkbox"/>	7	Ariya WiredAOS-S Dot1x	RADIUS	802.1X Wired	✓
8.	<input type="checkbox"/>	8	Ariya Wired-AOS-S MAC Auth	RADIUS	MAC Authentication	✗
9.	<input type="checkbox"/>	9	Ariya Wired-AOS-S MAC Auth-DUR	RADIUS	MAC Authentication	✓
10.	<input type="checkbox"/>	10	Ariya Wired-AOS-S GuestWebAuth	WEBAUTH	Web-based Authentication	✗
11.	<input type="checkbox"/>	11	Ariya Wired-AOS-S GuestWebAuth-DUR	WEBAUTH	Web-based Authentication	✓

Here are the details of “Wired-AOS-S MAC Auth-DUR”

Services - Ariya Wired-AOS-S MAC Auth-DUR

Summary	Service	Authentication	Authorization	Roles	Enforcement
Name: Ariya Wired-AOS-S MAC Auth-DUR					
Description: MAC-based Authentication Service					
Type: MAC Authentication					
Status: Enabled					
Monitor Mode: <input type="checkbox"/> Enable to monitor network access without enforcement					
More Options: <input checked="" type="checkbox"/> Authorization <input type="checkbox"/> Audit End-hosts <input type="checkbox"/> Profile Endpoints <input type="checkbox"/> Accounting Proxy					
Service Rule					
Matches <input type="radio"/> ANY or <input checked="" type="radio"/> ALL of the following conditions:					
	Type	Name	Operator	Value	
1.	Radius:IETF	NAS-Port-Type	BELONGS_TO	Ethernet (15), Wireless-802.11 (19)	 
2.	Radius:IETF	Service-Type	BELONGS_TO	Login-User (1), Call-Check (10)	 
3.	Connection	Client-Mac-Address	EQUALS	%{Radius:IETF:User-Name}	 
4.	Radius:IETF	Connect-Info	CONTAINS	CONNECT	 
5.	Click to add...				

Summary	Service	Authentication	Authorization	Roles	Enforcement
Authentication Methods: [Allow All MAC AUTH]					
<div> <div>Move Up ↑</div> <div>Move Down ↓</div> <div>Remove</div> <div>View Details</div> <div>Modify</div> </div>					
--Select to Add--					
Authentication Sources: [Endpoints Repository] [Local SQL DB]					
<div> <div>Move Up ↑</div> <div>Move Down ↓</div> <div>Remove</div> <div>View Details</div> <div>Modify</div> </div>					
--Select to Add--					
Strip Username Rules: <input type="checkbox"/> Enable to specify a comma-separated list of rules to strip username prefixes or suffixes					

Summary	Service	Authentication	Authorization	Roles	Enforcement
Authorization Details:					
Authorization sources from which role mapping attributes are fetched (for each Authentication Source)					
Authentication Source		Attributes Fetched From			
1.	[Endpoints Repository] [Local SQL DB]	[Endpoints Repository] [Local SQL DB]			
Additional authorization sources from which to fetch role-mapping attributes -					
<div> <div>[Insight Repository] [Local SQL DB]</div> <div>[Time Source] [Local SQL DB]</div> <div>[Guest User Repository] [Local SQL DB]</div> <div>[Guest Device Repository] [Local SQL DB]</div> <div>--Select to Add--</div> </div>					
<div> <div>Remove</div> <div>View Details</div> <div>Modify</div> </div>					
Add New Authentication Source					

Summary	Service	Authentication	Authorization	Roles	Enforcement
Role Mapping Policy:		Ariya Wired-AOS-S-MAC Auth-Role-Mapping			Modify Add New Role Mapping Policy
Role Mapping Policy Details					
Description:					
Default Role:	[Other]				
Rules Evaluation Algorithm:	evaluate-all				
Conditions	Role				
1. (Authorization:[Endpoints Repository]:Unique-Device-Count EXISTS) AND (Date:Date-Time LESS_THAN %{Endpoint:MAC-Auth Expiry})	[MAC Caching]				
2. (Endpoint:Guest Role ID EQUALS 1)	[Contractor]				
3. (Endpoint:Guest Role ID EQUALS 2)	[Guest]				
4. (Endpoint:Guest Role ID EQUALS 3)	[Employee]				
5. (Authorization:[Endpoints Repository]:Status EQUALS known) OR (Endpoint:HPE_CompanyAsset EQUALS true)	HPE_CompanyAsset				

Summary	Service	Authentication	Authorization	Roles	Enforcement
Use Cached Results:		<input type="checkbox"/> Use cached Roles and Posture attributes from previous sessions			
Enforcement Policy:		Ariya Wired-AOS-S MAC-Auth EnfmentPolicy-DUR			Modify Add New Enforcement Policy
Enforcement Policy Details					
Description:					
Default Profile:	Ariya DUR-Guest-CP				
Rules Evaluation Algorithm:	first-applicable				
Conditions	Enforcement Profiles				
1. (Tips:Role EQUALS HPE_CompanyAsset)	Ariya Wired-AOS-S-CorpDevice				
2. (Tips:Role MATCHES_ALL [MAC Caching] [User Authenticated] [Guest])	Ariya DUR-MAC-Auth, Ariya Return-Endpoint-Username				
3. (Tips:Role EQUALS [MAC Caching]) AND (Endpoint:Guest Role ID EQUALS AD-User)	Ariya Wired-AOS-S-AD-Guest, Ariya Return-Endpoint-Username				

Now when we a guest users connects to port4 of the switch, there will be a MAC auth and the default enforcement profile will use DUR-CP to send the captive portal redirection configuration to the switch.

Here is the Access tracker

Summary	Input	Output	Accounting	RADIUS CoA
Login Status:	ACCEPT			
Session Identifier:	R00000005-01-5c3aaef4			
Date and Time:	Jan 13, 2019 14:22:28 AEDT			
End-Host Identifier:	f0-de-f1-64-0a-82 (Computer / Windows / Windows)			
Username:	f0def1640a82			
Access Device IP/Port:	192.168.1.248:4 (Aruba-2930F-Lab2 / Hewlett-Packard-Enterprise)			
System Posture Status:	UNKNOWN (100)			
Policies Used -				
Service:	Ariya Wired-AOS-S MAC Auth-DUR			
Authentication Method:	MAC-AUTH			
Authentication Source:	None			
Authorization Source:	[Guest User Repository], [Guest Device Repository], [Endpoints Repository], [Insight Repository], [Time Source]			
Roles:	[Other], [User Authenticated]			
Enforcement Profiles:	Ariya DUR-Guest-CP			

Summary	Input	Output	Accounting	RADIUS CoA
Enforcement Profiles:	Ariya DUR-Guest-CP			
System Posture Status:	UNKNOWN (100)			
Audit Posture Status:	UNKNOWN (100)			
RADIUS Response				
Radius:Hewlett-Packard-Enterprise:HPE-CPPM-Role		Ariya_DUR_Guest_CP-3021-7 class ipv4 DUR-DHCP 10 match udp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 67 exit class ipv4 DUR-IP-ANY-ANY 10 match ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 exit class ipv4 DUR-WEB-TRAFFIC 10 match tcp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 80 20 match tcp 0.0.0.0 255.255.255.255 0.0.0.0		

And this is what we see on the switch.

```
Aruba-2930F-Lab2# sh user-role
Downloaded user roles are preceded by *
```

User Roles

```
Enabled      : Yes
Initial Role : denyall
```

Type	Name
-----	-----
local	Exec
local	TEST
local	GUEST
local	Staff
predefined	denyall
local	AD-Guest
local	Employee
local	Students
local	CORP-USER
local	InstantAP
local	CORP-DEVICE
local	InstantAP-1x
local	Critical-role
local	MAC-AUTH-CORP
local	CAPTIVE-PORTAL
downloaded	*Ariya_DUR_Staff-3035-2
downloaded	*Ariya_DUR_Guest_CP-3021-7
downloaded	*Ariya_DUR_MAC_Auth-3022-4

```
Aruba-2930F-Lab2#
Aruba-2930F-Lab2#
Aruba-2930F-Lab2# sh port-access client
Downloaded user roles are preceded by *
```

Port Access Client Status

Port	Client Name	MAC Address	IP Address	User Role	Type	VLAN
-----	-----	-----	-----	-----	-----	-----
4		f0def1-640a82	n/a		8021X	10
4	f0def1640a82	f0def1-640a82	n/a	*Ariya_DUR_Gue...	MAC	10

```
Aruba-2930F-Lab2#
```

As before the user will get redirected to the captive portal page and after the user uses cpguser credentials, it will see a wait for 30 sec.



And as before the WEBAUTH authentication comes in

#	Server	Source	Username	Service	Login Status	Request Timestamp
1.	192.168.1.94	RADIUS	cpguser	Ariya Wired-AOS-S MAC Auth-DUR	ACCEPT	2019/01/13 14:25:19
2.	192.168.1.94	WEBAUTH	cpguser	Ariya Wired-AOS-S GuestWebAuth-DUR	ACCEPT	2019/01/13 14:25:00
3.	192.168.1.94	RADIUS	f0def1640a82	Ariya Wired-AOS-S MAC Auth-DUR	ACCEPT	2019/01/13 14:22:28

This authenticates the cpguser and then bounces the switch port.

Summary	Input	Output
Enforcement Profiles:	Ariya AOS-S GuestMAC-Caching, Ariya AOS-S MAC Caching Expire Post Login, [Update Endpoint Known], [ArubaOS Switching - Bounce Switch Port]	
System Posture Status:	UNKNOWN (100)	
Audit Posture Status:	UNKNOWN (100)	
RADIUS Response		
Endpoint:Guest Role ID	2	
Endpoint:MAC-Auth Expiry	2019-03-30 16:32:45	
Endpoint:Username	cpguser	
Expire-Time-Update:GuestUser	0	
Radius:Hewlett-Packard-Enterprise:HPE-Port-Bounce-Host	12	
Radius:IETF:Calling-Station-Id	f0-de-f1-64-0a-82	
Radius:IETF:NAS-IP-Address	192.168.1.248	
Radius:IETF:NAS-Port	4	
Radius:IETF:User-Name	f0def1640a82	
Status-Update:Endpoint	Known	

Lastly this will generate the third authentication, in which the DUR of Guest user is sent to the switch.

Summary	Input	Output	Accounting
Login Status:	ACCEPT		
Session Identifier:	R00000006-01-5c3aaf9f		
Date and Time:	Jan 13, 2019 14:25:19 AEDT		
End-Host Identifier:	f0-de-f1-64-0a-82 (Computer / Windows / Windows)		
Username:	cpguser		
Access Device IP/Port:	192.168.1.248:4 (Aruba-2930F-Lab2 / Hewlett-Packard-Enterprise)		
System Posture Status:	UNKNOWN (100)		
Policies Used -			
Service:	Ariya Wired-AOS-S MAC Auth-DUR		
Authentication Method:	MAC-AUTH		
Authentication Source:	Local:localhost		
Authorization Source:	[Guest User Repository], [Guest Device Repository], [Endpoints Repository], [Insight Repository], [Time Source]		
Roles:	[Guest], [MAC Caching], [User Authenticated]		
Enforcement Profiles:	Ariya DUR-MAC-Auth, Ariya Return-Endpoint-Username		

Summary	Input	Output	Accounting
		<pre> exit class ipv4 DUR-Internet 10 match ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 exit policy user DUR-Guest 10 class ipv4 DUR-Guest-DHCP action permit 20 class ipv4 DUR-Guest-DNS action permit 30 class ipv4 DUR-Internal-Net action deny 40 class ipv4 DUR-Internet action permit exit aaa authorization user-role name DUR-Guest reauth-period 3600 vlan-id 10 policy DUR-Guest exit </pre>	
Radius:IETF:User-Name		cpguser	

And this is what we see on the LAN switch

```
Aruba-2930F-Lab2# sh port-access client
Downloaded user roles are preceded by *
```

Port Access Client Status

Port	Client Name	MAC Address	IP Address	User Role	Type	VLAN
4	cpguser	f0def1-640a82	10.10.10.101	*Ariya_DUR_MAC...	MAC	10

```
Aruba-2930F-Lab2# sh port-access client det
```

Port Access Client Status Detail

Client Base Details :

Port	: 4	Authentication Type	: mac-based
Client Status	: authenticated	Session Time	: 544 seconds
Client Name	: cpguser	Session Timeout	: 3600 seconds
MAC Address	: f0def1-640a82		
IP	: 10.10.10.101		
Auth Order	: Mac-Auth, 8021x		
Auth Priority	: 8021x, Mac-Auth		
LMA Fallback	: Disabled		

Downloaded user roles are preceded by *

User Role Information

Name	: *Ariya_DUR_MAC_Auth-3022-4
Type	: downloaded
Reauthentication Period (seconds)	: 3600
Cached Reauth Period (seconds)	: 0
Logoff Period (seconds)	: 300
Untagged VLAN	: 10
Tagged VLANs	:
Captive Portal Profile	:
Policy	: DUR-Guest Ariya DUR MAC Auth-3022-4

Statements for policy "DUR-Guest_Ariya_DUR_MAC_Auth-3022-4"

```
policy user "DUR-Guest_Ariya_DUR_MAC_Auth-3022-4"
```

```

10 class ipv4 "DUR-Guest-DHCP_Ariya_DUR_MAC_Auth-3022-4" action permit
20 class ipv4 "DUR-Guest-DNS_Ariya_DUR_MAC_Auth-3022-4" action permit
30 class ipv4 "DUR-Internal-Net_Ariya_DUR_MAC_Auth-3022-4" action deny
40 class ipv4 "DUR-Internet_Ariya_DUR_MAC_Auth-3022-4" action permit
exit

```

```

Statements for class IPv4 "DUR-Guest-DHCP_Ariya_DUR_MAC_Auth-3022-4"
class ipv4 "DUR-Guest-DHCP_Ariya_DUR_MAC_Auth-3022-4"
    10 match udp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 67
    exit

Statements for class IPv4 "DUR-Guest-DNS_Ariya_DUR_MAC_Auth-3022-4"
class ipv4 "DUR-Guest-DNS_Ariya_DUR_MAC_Auth-3022-4"
    10 match udp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 53
    exit

Statements for class IPv4 "DUR-Internal-Net_Ariya_DUR_MAC_Auth-3022-4"
class ipv4 "DUR-Internal-Net_Ariya_DUR_MAC_Auth-3022-4"
    10 match ip 0.0.0.0 255.255.255.255 10.10.30.0 0.0.0.255
    exit

Statements for class IPv4 "DUR-Internet_Ariya_DUR_MAC_Auth-3022-4"
class ipv4 "DUR-Internet_Ariya_DUR_MAC_Auth-3022-4"
    10 match ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
    exit

Tunnelednode Server Redirect      : Disabled
Secondary Role Name               :
Device Attributes                  : Disabled

```

Aruba-2930F-Lab2#

12.6 DUR with Instant APs – dot1x

When using DUR for Aruba Instant APs we need to first configure a DUR enforcement profile.

Summary

Profile

Attributes

Profile:

Name:	Ariya DUR-IAP-1x
Description:	
Type:	RADIUS
Action:	Accept
Device Group List:	-
Product:	ArubaOS-Switch

Attributes:

Type	Name	Value
1.	Radius:Hewlett-Packard-Enterprise	HPE-CPPM-Role = class ipv4 IP-ANY-ANY match ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 exit policy user InstantAP class ipv4 "IP-ANY-ANY" action permit exit
		aaa authorization user-role name InstantAP-1x policy "InstantAP" vlan-id 10 vlan-id-tagged 20 device port-mode

Here is the details of the attribute value

```

class ipv4 IP-ANY-ANY
match ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
exit

policy user InstantAP
    class ipv4 "IP-ANY-ANY" action permit
    exit

aaa authorization user-role name InstantAP-1x
    policy "InstantAP"

```

```

vlan-id 10
  vlan-id-tagged 20
  device
    port-mode
    exit
exit

```

Now we need to modify the dot1x service to reflect the above enforcement profile.

Services - Ariya WiredAOS-S Dot1x

Summary	Service	Authentication	Roles	Enforcement
Use Cached Results:	<input type="checkbox"/> Use cached Roles and Posture attributes from previous sessions			
Enforcement Policy:	<div>Ariya Wired-AOS-S Dot1xEnforcementPolicy</div> <div>Modify</div>			Add New Enforcement Policy
Enforcement Policy Details				
Description:				
Default Profile:	[Deny Access Profile]			
Rules Evaluation Algorithm:	first-applicable			
Conditions	Enforcement Profiles			
1. (Authorization:AriyaAD:memberOf CONTAINS staff)	Ariya DUR-Staff, [Update Endpoint Known]			
2. (Authorization:AriyaAD:memberOf CONTAINS Stude)	Ariya DUR-Student, [Update Endpoint Known]			
3. (Authorization:AriyaAD:memberOf CONTAINS exec)	Ariya DUR-Exec, Ariya HPE_Asset update, [Update Endpoint Known]			
4. (Tips:Role EQUALS InstantAP)	Ariya DUR-IAP-1x			

We will connect an IAP to port 4 of the switch and check the ClearPass access tracker

Summary	Input	Output	Accounting
Login Status:	ACCEPT		
Session Identifier:	R0000000b-01-5c3ab92e		
Date and Time:	Jan 13, 2019 15:06:06 AEDT		
End-Host Identifier:	20-4c-03-23-a7-98 (Access Points / Aruba / Aruba IAP)		
Username:	InstantAP		
Access Device IP/Port:	192.168.1.248:4 (Aruba-2930F-Lab2 / Hewlett-Packard-Enterprise)		
System Posture Status:	UNKNOWN (100)		
Policies Used -			
Service:	Ariya WiredAOS-S Dot1x		
Authentication Method:	EAP-PEAP,EAP-MSCHAPv2		
Authentication Source:	Local:localhost		
Authorization Source:	[Local User Repository]		
Roles:	InstantAP, [User Authenticated]		
Enforcement Profiles:	Ariya DUR-IAP-1x		
Service Monitor Mode:	Disabled		

SummaryInputOutputAccounting

RADIUS Response

Radius:Hewlett-Packard-Enterprise:HPE-CPPM-Role

Ariya_DUR_IAP_1x-3040-2
class ipv4 IP-ANY-ANY
match ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
exit

policy user InstantAP
class ipv4 "IP-ANY-ANY" action permit
exit

aaa authorization user-role name InstantAP-1x
policy "InstantAP"
vlan-id 10
vlan-id-tagged 20
device
port-mode
exit
exit

From the switch we can see this

```
Aruba-2930F-Lab2# sh user-role
Downloaded user roles are preceded by *
```

User Roles

Enabled : Yes

Initial Role : denyall

Type	Name
local	Exec
local	TEST
local	GUEST
local	Staff
predefined	denyall
local	AD-Guest
local	Employee
local	Students
local	CORP-USER
local	InstantAP
local	CORP-DEVICE
local	InstantAP-1x
local	Critical-role
local	MAC-AUTH-CORP
local	CAPTIVE-PORTAL
downloaded	*Ariya_DUR_Staff-3035-2
downloaded	*Ariya_DUR_IAP_1x-3040-2
downloaded	*Ariya_DUR_Guest_CP-3021-7
downloaded	*Ariya_DUR_MAC_Auth-3022-4

```
Aruba-2930F-Lab2#
Aruba-2930F-Lab2# sh port-access client
Downloaded user roles are preceded by *
```

Port Access Client Status

Port	Client Name	MAC Address	IP Address	User Role	Type	VLAN
4	InstantAP	204c03-23a798	10.10.10.100	*Ariya_DUR_IAP...	8021X	20, 10

```
Aruba-2930F-Lab2#
```

12.7 DUR with Instant APs – Profiling

Following on with the same concepts, we'll now disable supplicant dot1x authentication for IAPs and now ClearPass will profile them and based on the fact that they are Instant APs, they will be pushed into their user-role. The enforcement profile will be DUR-IAP

#	Name ▲	Type	Description
1.	<input type="checkbox"/> Ariya DUR-Exec	RADIUS	
2.	<input type="checkbox"/> Ariya DUR-Guest-CP	RADIUS	
3.	<input type="checkbox"/> Ariya DUR-IAP	RADIUS	
4.	<input type="checkbox"/> Ariya DUR-IAP-1x	RADIUS	
5.	<input type="checkbox"/> Ariya DUR-MAC-Auth	RADIUS	
6.	<input type="checkbox"/> Ariya DUR-Staff	RADIUS	
7.	<input type="checkbox"/> Ariya DUR-Std	RADIUS	
8.	<input type="checkbox"/> Ariya DUR-Student	RADIUS	

and this needs to be reference in the MAC auth service policy

Services - Ariya Wired-AOS-S MAC Auth-DUR

Summary	Service	Authentication	Authorization	Roles	Enforcement
Use Cached Results: <input type="checkbox"/> Use cached Roles and Posture attributes from previous sessions					
Enforcement Policy:		Ariya Wired-AOS-S MAC-Auth EnfmentPolicy-DUR <div>Modify</div>			Add New Enforcement Policy
Enforcement Policy Details					
Description:					
Default Profile:		Ariya DUR-Guest-CP			
Rules Evaluation Algorithm:		first-applicable			
Conditions			Enforcement Profiles		
1. (Tips:Role EQUALS HPE_CompanyAsset)			Ariya Wired-AOS-S-CorpDevice		
2. (Tips:Role MATCHES_ALL [MAC Caching] [User Authenticated] [Guest])			Ariya DUR-MAC-Auth, Ariya Return-Endpoint-Username		
3. (Tips:Role EQUALS [MAC Caching]) AND (Endpoint:Guest Role ID EQUALS AD-User)			Ariya Wired-AOS-S-AD-Guest, Ariya Return-Endpoint-Username		
4. (Authorization:[Endpoints Repository]:Device Name EQUALS Aruba IAP)			Ariya DUR-IAP		

So now our ClearPass services are as shown here.

7.	<input type="checkbox"/>	7	Ariya WiredAOS-S Dot1x	RADIUS	802.1X Wired	✓
8.	<input type="checkbox"/>	8	Ariya Wired-AOS-S MAC Auth	RADIUS	MAC Authentication	✗
9.	<input type="checkbox"/>	9	Ariya Wired-AOS-S MAC Auth-DUR	RADIUS	MAC Authentication	✓
10.	<input type="checkbox"/>	10	Ariya Wired-AOS-S GuestWebAuth	WEBAUTH	Web-based Authentication	✗
11.	<input type="checkbox"/>	11	Ariya Wired-AOS-S GuestWebAuth-DUR	WEBAUTH	Web-based Authentication	✓

Once we have disabled supplicant dot1x on IAP, we need to reboot it.

Summary	Input	Output	Accounting
Login Status:	ACCEPT		
Session Identifier:	R0000000c-01-5c3abb92		
Date and Time:	Jan 13, 2019 15:16:18 AEDT		
End-Host Identifier:	20-4c-03-23-a7-98 (Access Points / Aruba / Aruba IAP)		
Username:	204c0323a798		
Access Device IP/Port:	192.168.1.248:4 (Aruba-2930F-Lab2 / Hewlett-Packard-Enterprise)		
System Posture Status:	UNKNOWN (100)		
Policies Used -			
Service:	Ariya Wired-AOS-S MAC Auth-DUR		
Authentication Method:	MAC-AUTH		
Authentication Source:	None		
Authorization Source:	[Guest User Repository], [Guest Device Repository], [Endpoints Repository], [Insight Repository], [Time Source]		
Roles:	[Other], [User Authenticated]		
Enforcement Profiles:	Ariya DUR-IAP		

SummaryInputOutputAccounting

RADIUS Response

Radius:Hewlett-Packard-Enterprise:HPE-CPPM-Role

Ariya_DUR_IAP-3039-2
class ipv4 IP-ANY-ANY
match ip 0.0.0.0 255.255.255.255 0.0.0.0
255.255.255.255
exit

policy user InstantAP
class ipv4 "IP-ANY-ANY" action permit
exit

aaa authorization user-role name InstantAP
policy "InstantAP"
vlan-id 10
vlan-id-tagged 20
device
port-mode
exit
exit

```
Aruba-2930F-Lab2# sh user-role
Downloaded user roles are preceded by *
```

User Roles

```
Enabled      : Yes
Initial Role : denyall
```

Type	Name
-----	-----
local	Exec
local	TEST
local	GUEST
local	Staff
predefined	denyall
local	AD-Guest
local	Employee
local	Students
local	CORP-USER
local	InstantAP
local	CORP-DEVICE
local	InstantAP-1x
local	Critical-role
local	MAC-AUTH-CORP
local	CAPTIVE-PORTAL
downloaded	*Ariya_DUR_IAP-3039-2
downloaded	*Ariya_DUR_Staff-3035-2
downloaded	*Ariya_DUR_IAP_1x-3040-2
downloaded	*Ariya_DUR_Guest_CP-3021-7
downloaded	*Ariya_DUR_MAC Auth-3022-4

```
Aruba-2930F-Lab2# sh port-access client
Downloaded user roles are preceded by *
```

Port Access Client Status

Port	Client Name	MAC Address	IP Address	User Role	Type	VLAN
-----	-----	-----	-----	-----	-----	-----
4	204c0323a798	204c03-23a798	10.10.10.100	*Ariya_DUR_IAP... MAC	MAC	20, 10

```
Aruba-2930F-Lab2#
```

This is to check the LAN switch resources.

Aruba-2930F-Lab2#

Aruba-2930F-Lab2# show access-list resources

Resource usage in Policy Enforcement Engine

Ingress Policy Enforcement Engine Rules

Resource usage in Policy Enforcement Engine

Ports	Rules	Rules Used									
	Available	ACL	QoS	IDM	VT	Mirr	PBR	OF	Other		
1-10	4080	0	0	0	0	0	0	0	0	0	0

Ingress Policy Enforcement Engine Meters

Ports	Meters	Meters Used									
	Available	ACL	QoS	IDM	VT	Mirr	PBR	OF	Other		
1-10	2047		0	0	0			0	0		

Ingress Policy Enforcement Engine Port Ranges

	Application											
	Port Ranges											
	Next-hops											
	Application Port Ranges Used											
	PBR Next-hops Used											
1-10	60	0	0	0		0	0	0	0	0	0	

Ingress Policy Enforcement Engine PBR Resources

Ports	PBR										
	Available	ACL	QoS	IDM	VT	Mirr	PBR	OF	Other		
1-10	1024						0			0	

3 of 32 Policy Engine management resources used.

Egress Policy Enforcement Engine Rules

Resource usage in Policy Enforcement Engine

Ports	Rules	Rules Used									
	Available	ACL	QoS	IDM	VT	Mirr	PBR	OF	Other		
1-10	2032	0	0	0	0	0	0	0	0	0	0

Egress Policy Enforcement Engine Meters

Ports	Meters	Meters Used									
	Available	ACL	QoS	IDM	VT	Mirr	PBR	OF	Other		
1-10	1023		0	0	0			0	0		

Egress Policy Enforcement Engine Port Ranges

Application		Application Port Ranges Used								
Ports	Port Ranges	Available	ACL	QoS	IDM	VT	Mirr	PBR	OF	Other
1-10		60	0	0	0		0	0	0	0

0 of 8 Policy Engine management resources used.

Key:

ACL = Access Control Lists

QoS = Device & Application Port Priority, QoS Policies, ICMP rate limits

IDM = Identity Driven Management

VT = Virus Throttling blocks

Mirr = Mirror Policies, Remote Intelligent Mirror endpoints

PBR = Policy Based Routing Policies

OF = OpenFlow

Other = Management VLAN, DHCP Snooping, ARP Protection, Jumbo IP-MTU, RA Guard, Control Plane Protection, Service Tunnel, ND Snooping, UWW, mDNS, tunneled-node-server, copp, ICMP rate-limit, Unknown Unicast rate-limit.

Resource usage includes resources actually in use, or reserved for future use by the listed feature. Internal dedicated-purpose resources, such as port bandwidth limits or VLAN QoS priority, are not included.

Here are the system Limits for DUR for various switch models.

System Limits in DUR	5400R (v2 and v3) /3810	2920/2930F/2930M
Total ACLs ("match" rules) per port (in all classes combined)	100	32
Total ACEs per ACL ("class" statements per policy)	100	100
Total ACEs ("class" statements) per port (in all policies combined)	4000	400
Total ACEs ("class" statements) per system (in all policies and in all ports combined)	~4k	~2k
Total user roles per system (irrespective of Stack/Standalone)	32	32